IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MISSOURI
SOUTHERN DIVISION

CHOICE ESCROW AND LAND TITLE, LLC,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 10-03531-CV-S-JTM
	)	
BANCORPSOUTH BANK,	)	
	)	
Defendant.	)	

SECOND AMENDED COMPLAINT

COMES NOW Plaintiff, Choice Escrow and Land Title, LLC ("Choice"), and for its Second Amended Complaint against Defendant, BancorpSouth Bank ("BancorpSouth"), states as follows:

Parties

1. Plaintiff Choice is a Missouri limited liability company, which operates as a land title and escrow business in Springfield, Missouri.

2. Defendant BancorpSouth is a Mississippi banking corporation with a principal place of business and headquarters in Tupelo, Mississippi, authorized to do business in Missouri, and doing business in Springfield, Missouri.

Choice of Law

3. Pursuant to Section 4A-507 of the Uniform Commercial Code (Miss. Code Ann. §75-4A-507 and Mo. Rev. Stat. §400.4A-507), the rights and obligations between Choice and BancorpSouth, regarding the issues and subjects of this lawsuit, are governed by the laws of the State of Mississippi.

4. The applicable Mississippi law is the Funds Transfer section of Mississippi's Uniform Commercial Code (Mississippi Code Annotated §§75-4A-101 et seq. (Rev. 2002)).

Unauthorized Acceptance of Fraudulent Wire Transfer

5. On March 17, 2010, BancorpSouth transferred $440,000.00 (Four Hundred Forty Thousand Dollars) out of an account Choice had with BancorpSouth, after BancorpSouth accepted an internet-based funds transfer payment order (the "Wire Transfer").

6. Choice's account with BancorpSouth, from which the Wire Transfer was made, was a trust account and an escrow disbursement account, identified as account number 0618003800.

7. The Wire Transfer was sent from BancorpSouth, as originator bank, to Bank of New York, as intermediary bank, for further transfer internationally to Popular Bank Public Co. Ltd. in the Republic of Cyprus, as beneficiary bank for the beneficiary, Brolaw Services, LTD.

8. Choice has never previously heard of, had contact with, done business with, transferred money to, or held money in escrow for Brolaw Services, LTD, or any individual or entity associated with Brolaw Services, LTD.

9. The Wire Transfer was not created, sent, approved, released, authorized, or ratified by Choice, or its members, managers, agents, representatives, officers, employees or any other person or entity in any way associated with Choice.

10. The Wire Transfer was created and sent by an unknown third party ("Hacker") with no affiliation or association with Choice, or actual or apparent authority to act on behalf of Choice.

11. The "Balance Statement For Trust Account--Account No. 0618003800", attached hereto and incorporated herein by reference as EXHIBIT 12, was created by BancorpSouth.

12. On March 17, 2010, Choice's said account had a current ledger balance of $349,352.20 (Three Hundred Forty-Nine Thousand Three Hundred Fifty-Two Dollars and Twenty Cents).

13. The Wire Transfer's "Facsimile Transmission Receipt", attached hereto and incorporated herein by reference as EXHIBIT 5, indicates the money transferred out of Choice's account was for "Invoice: equipment".

14. Prior to the Wire Transfer, funds from Choice's said account with BancorpSouth had never been wired or transferred to pay an invoice or to purchase equipment.

15. On or about November 11, 2009, Jim Payne, a member of Choice, sent an email to Ashley Kester, an employee of BancorpSouth, expressing that Choice desired to limit wire transfers to foreign banks.

16. On or about November 13, 2009, Ashley Kester sent an email to Jim Payne and Robin Fleming, an employee of BancorpSouth, indicating BancorpSouth was unable to stop foreign wires and that Choice should consider Dual Control.

17. Prior to the Wire Transfer, funds from Choice's said account with BancorpSouth had never been wired or transferred to an international bank or an international beneficiary.

18. Prior to the Wire Transfer, Choice had never authorized a transfer of funds out of its said BancorpSouth account to an international bank or an international beneficiary.

19. On March 17, 2010, Choice notified BancorpSouth, via email from Brooke Black, an employee of Choice, to Robin Fleming, an employee of BancorpSouth, that Choice was unable to access BancorpSouth's internet-based funds transfer website, InView, due to website maintenance.

20. On March 17, 2010, no maintenance was performed by BancorpSouth, its vendors, agents or representatives, on InView which would have rendered said website inaccessible to its customers.

21. BancorpSouth did not recover any of the $440,000.00 in funds transferred from Choice's account on March 17, 2010, from the Wire Transfer.

22. BancorpSouth has not refunded or repaid any of the funds transferred from Choice's account on March 17, 2010, from the Wire Transfer.

Guidance on Internet Banking Security Procedures

23. The Federal Financial Institutions Examination Council ("FFIEC") is a formal interagency body empowered to prescribe uniform principles and standards for the federal examination of financial institutions, and was established in 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978.

24. The regulatory agencies which comprise the membership of the FFIEC are (1) the Board of Governors of the Federal Reserve System, (2) the National Credit Union

Administration, (3) the Office of the Comptroller of the Currency, (4) the Office of Thrift Supervision, and (5) the Federal Deposit Insurance Corporation ("FDIC").

25. The FDIC supervises or regulates BancorpSouth.

26. BancorpSouth is one of the financial institutions for which the FFIEC prescribes principles and standards.

27. In 2005, the FFIEC issued guidance, entitled "Authentication in an Internet Banking Environment" ("2005 Guidance"), attached hereto and incorporated herein by reference as EXHIBIT 1.

28. The 2005 Guidance, inter alia, indicated the risk management controls necessary as of 2005 to authenticate customers accessing internet-based financial services.

29. In 2006, the FFIEC issued a Frequently Asked Questions memorandum ("2006 FAQ"), attached hereto and incorporated herein by reference as EXHIBIT 2.

30. The 2006 FAQ, inter alia, was issued to assist financial institutions in understanding the 2005 Guidance and its scope.

31. Pursuant to the 2005 Guidance (Exhibit 1) and 2006 FAQ (Exhibit 2), BancorpSouth was encouraged to monitor, evaluate, asses and adjust its security programs in light of changes in technology, the sensitivity of customer information, and internal and external threats to information.

32. In April of 2007, the FDIC issued a Financial Institution Letter entitled "Supervisory Policy on Identity Theft" ("FIL-32-2007"). FIL-32-2007 is attached hereto and incorporated herein by reference as EXHIBIT 3.

33. FIL-32-2007 (Exhibit 3), inter alia, stated the FDIC's expectations that the institutions under its supervision should detect, prevent and mitigate the effects of identity theft in order to protect consumers and to help ensure safe and sound operations.

34. FIL-32-2007 (Exhibit 3), inter alia, stated that FDIC-supervised banks have an affirmative and continuing obligation to protect the privacy of customers' non-public personal information and that despite general strong controls and practices by financial institutions, methods for stealing personal data and committing fraud with that data are continuously evolving.

35. In August of 2009, the FDIC issued a Special Alert with the subject "Fraudulent Electronic Funds Transfers (EFTs)" ("SA-147-2009"). SA-147-2009 is attached hereto and incorporated herein by reference as EXHIBIT 4.

36. SA-147-2009 (Exhibit 4), inter alia, warned FDIC-supervised banks of the increased number of fraudulent electronic funds transfers resulting from compromised user login credentials and directed its financial institutions to the 2005 Guidance and the 2006 FAQ as references for information on security procedures for high-risk transactions.

37. BancorpSouth had adequate notice of, or knew or should have known about, the 2005 Guidance (Exhibit 1), 2006 FAQ (Exhibit 2), FIL-32-2007 (Exhibit 3) and SA-147-2009 (Exhibit 4), and the information contained therein, prior to March 17, 2010.

38. Pursuant to the 2005 Guidance (Exhibit 1), 2006 FAQ (Exhibit 2), FIL-32-2007 (Exhibit 3) and SA-147-2009 (Exhibit 4), inter alia, the prevailing standards of good banking practice for internet banking constantly evolve as internet-based threats to customer accounts become known to the banking industry.

39. The prevailing standard for good banking practice for FFIEC and FDIC regulated or supervised banks is for said banks to perform periodic risk-assessments and to implement security procedure which combat or protect against known internet-based threats to customer accounts.

40. In 2011, the FFIEC issued supplemental guidance, entitled "Supplement to Authentication in an Internet Banking Environment" ("2011 Supplement"), attached hereto and incorporated herein by reference as EXHIBIT 13.

41. The 2011 Supplement (Exhibit 13) was issued by the FFIEC more than one year after the Wire Transfer.

42. The 2011 Supplement (Exhibit 13), inter alia, clarified the 2005 Guidance and its scope and that the concept of customer authentication described in the 2005 Guidance is broad and includes more than the initial authentication of the customer when it connects to the financial institution at login

43. The 2011 Supplement (Exhibit 13), inter alia, stated that since 2005, there have been significant changes in the (internet banking authentication) threat landscape.

44. While the 2011 Supplement (Exhibit 13) was not issued prior to the Wire Transfer, there will likely be evidentiary support after a reasonable opportunity for further investigation or discovery that the threats, controls and ineffectiveness of certain authentication methods it addresses were known in the banking industry prior March 17, 2010.

<u>BancorpSouth's Internet-Based Funds Transfer Security Procedures</u>

45. On and before March 17, 2010, BancorpSouth offered Choice only two security procedures for internet-based funds transfers, Dual Control or Single Control.

46. On and before March 17, 2010, "Dual Control" was the security procedure BancorpSouth had available and offered to Choice that BancorpSouth held out to be its best security procedure for internet-based funds transfers.

47. Dual Control required a BancorpSouth customer to have one user ID and Password to "create" a wire transfer and another user ID and password to "approve" and/or "release" the same wire transfer.

48. Dual Control required more than one person to initiate and complete the wire transfer process.

49. On and before March 17, 2010, "Single Control" was the security procedure BancorpSouth had available and offered to Choice that BancorpSouth held out to be a lesser security procedure than Dual Control for internet-based funds transfers.

50. Single Control required a BancorpSouth customer to have only one user ID and Password to "create" a wire transfer and to "approve" and/or "release" the same wire transfer.

51. Due to the smaller size of its business and operations, Choice often had only one person available to create, approve and release a wire transfer.

52. Choice used Single Control, since it was the only suitable and feasible option that BancorpSouth offered and made available to Choice on and before March 17, 2010, in that Dual Control required more than one person to initiate and complete the wire transfer process.

53. Choice and BancorpSouth entered into the following described documents (collectively referred to as the "Agreement Documents"):

a. Funds Transfer Agreement (attached hereto for purpose of identification only as EXHIBIT 6; Plaintiff does not intend to adopt or incorporate Exhibit 6, or the language contained therein, for all purposes);

b. Business Services Agreement (attached hereto for purpose of identification only as EXHIBIT 7; Plaintiff does not intend to adopt or incorporate Exhibit 7, or the language contained therein, for all purposes);

c. InView Automated Information Reporting Service Implementation Form/Addendum to Business Services Agreement (attached hereto for purpose of identification only as EXHIBIT 8; Plaintiff does not intend to adopt or incorporate Exhibit 8, or the language contained therein, for all purposes);

d. Deposit Account Terms and Conditions Agreement (attached hereto for purpose of identification only as EXHIBIT 9; Plaintiff does not intend to adopt or incorporate Exhibit 9, or the language contained therein, for all purposes);

e. Waiver Consent--InView Wire Module Dual Control (attached hereto for purpose of identification only as EXHIBIT 10; Plaintiff does not intend to adopt or incorporate Exhibit 10, or the language contained therein, for all purposes);

f. InView Wire Transfer User Security Form (attached hereto for purpose of identification only as EXHIBIT 11; Plaintiff does not intend to adopt or incorporate Exhibit 11 or the language contained therein, for all purposes).

54. To the extent any agreements or contracts by and/or between Choice and BancorpSouth, including but not limited to the Agreement Documents, purport to establish or pre-establish the commercial reasonableness of BancorpSouth's security procedures, or BancorpSouth's good faith, or what conduct is required of BancorpSouth to comply with good

faith, with regard to (and before, during and after) the Wire Transfer, said documents are unenforceable, void and/or invalid in that they are:

a. Unconscionable, substantively and/or procedurally; and/or

b. Adhesion, form agreements, which contain terms which are unreasonable, unexpected and/or unfair; and/or

c. In violation of Miss. Code Ann. §75-4A-202(f).

Count I --- Violation of and/or Failure to Comply with

Miss. Code Ann. §75-4A-202 (Rev. 2002)

55. Plaintiff incorporates by reference and re-alleges herein paragraphs 1 through 54, inclusive, as if the same were more fully set forth herein.

56. The Wire Transfer was, in fact, not authorized by Choice, or its members, managers, agents, representatives, officers or employees.

57. The Wire Transfer was, in fact, not authorized by a person or entity with actual or apparent agency authority from Choice.

58. Choice did not, nor did a person or entity with actual or apparent agency authority from Choice, engage in conduct which would cause Choice to be bound by the unauthorized Wire Transfer or which would estop Choice from denying the Wire Transfer was authorized.

59. Choice expressed to BancorpSouth its wish, requirement and/or instruction that its said account with BancorpSouth be a trust account and an escrow disbursement account, which was to be used solely to transfer funds for home loans or for payoffs related to commercial or residential real estate transactions.

60. Choice expressed to Bancorpsouth its wish, requirement and/or instruction that its account's current ledger balance govern whether or not BancorpSouth could accept a wire transfer.

61. Choice by email on or about November 11, 2009, from Jim Payne to Ashley Kester, expressed to BancorpSouth its wish, requirement and/or instruction that BancorpSouth limit transfers to foreign banks.

62. BancorpSouth had adequate notice of Choice's wishes, requirements and/or instructions described herein, through emails, letters, documents, agreements, contracts, conversations and/or other communications by and between representatives of Choice and representatives of BancorpSouth, prior to March 17, 2010.

63. BancorpSouth had adequate notice of, and/or knew or should have known, Choice's circumstances, including that:

a. Choice's current ledger balance on March 17, 2010, was less than the amount of the Wire Transfer;

b. Choice had never previously (i.e. with no frequency) transferred an amount greater than was in its account's current ledger balance;

c. Choice had never previously (i.e. with no frequency) sent payment orders to pay invoices or to purchase equipment;

d. Choice had never previously (i.e. with no frequency) sent or authorized a payment order to an international bank;

e. Choice had never previously (i.e. with no frequency) sent or authorized a payment order to Brolaw Services, LTD;

f. Choice had never previously (i.e. with no frequency) sent or authorized a payment order to an international beneficiary.

64. BancorpSouth is not a small, community bank.

65. BancorpSouth is a large and sophisticated, multi-state bank, which has been in operation for over 100 years.

66. BancorpSouth should have made available to Choice up-to-date (if not state-of-the-art) security procedures which were more complex, sophisticated and commercially reasonable than Dual Control and Single Control.

67. The only purported security Dual Control offered that Single Control did not offer was one additional ID and Password.

68. Dual Control, the only alternative security procedure offered to Choice by BancorpSouth, was not commercially reasonable for Choice and was not suitable or feasible for Choice.

69. Dual Control would not have complied with, or accommodated for, Choice's wishes, requirements, instructions and/or circumstances described herein.

70. Dual Control would not have limited transfers to foreign banks.

71. Choice, by email on or about November 13, 2009, from Jim Payne to Ashley Kester, expressed to BancorpSouth Choice's wish, requirement, instruction and/or circumstance that two separate IDs and Passwords, as Dual Control required, would not be feasible or suitable for Choice, since often there is only one person in Choice's office who must create, approve and release wire transfers.

72. Choice did not enter into any agreements or contracts with BancorpSouth, including but not limited to the Agreement Documents, in which Choice expressly agreed in

writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by BancorpSouth in compliance with the security procedures chosen by Choice.

73. Choice's wishes, requirements and/or instructions regarding its escrow disbursement account, and regarding its security procedure, do not violate any written agreement between Choice and BancorpSouth, including but not limited to the Agreement Documents.

74. The Wire Transfer was the type of high-risk transaction about which the 2005 Guidance (Exhibit 1), 2006 FAQ (Exhibit 2), FIL-32-2007 (Exhibit 3), and SA-247-2009 (Exhibit 4) warned BancorpSouth for which single-factor authentication would be inadequate as the only security procedure.

75. Single Control required one password to be entered, which is a single-factor authentication that is not a commercially reasonable security procedure for high-risk transactions such as the Wire Transfer.

76. Dual Control required two passwords to be entered, which is a single-factor authentication that is not a commercially reasonable security procedure for high-risk transactions such as the Wire Transfer.

77. Prior to March 17, 2010, the existence of the internet-banking attacks commonly referred to as Man-in-the-Middle and Man-in-the-Browser were known in the banking industry and/or the internet-banking security industry.

78. On and prior to March 17, 2010, BancorpSouth did not provide to Choice security procedures designed to protect against Man-in-the-Middle and Man-in-the-Browser attacks.

79. On and prior to March 17, 2010, BancorpSouth should have provided security procedures which protected against Man-in-the-Middle and Man-in-the-Browser attacks, as was the standard of good banking practice.

80. The prevailing standard of good banking practice applicable to BancorpSouth on and prior to March 17, 2010, required more adequate and commercially reasonable security procedures than BancorpSouth offered and provided to Choice on and prior to March 17, 2010.

81. BancorpSouth accepted the Wire Transfer for "Invoice: equipment", despite the fact that Choice's account with BancorpSouth was an escrow disbursement account used solely to transfer funds for home loans or for payoffs related to commercial or residential real estate transactions, and that Choice had never previously (i.e. with no frequency) transferred funds to pay an invoice or to purchase equipment.

82. BancorpSouth accepted the Wire Transfer to Popular Bank Public Co. Ltd. in the Republic of Cyprus, despite Choice's wish, requirement and/or instruction that BancorpSouth limit and disable transfers to foreign banks, and despite Choice having never previously (i.e. with no frequency) transferred funds to an international bank.

83. BancorpSouth accepted the Wire Transfer to Brolaw Services, LTD, despite Choice having never previously (i.e. with no frequency) transferring funds to Brolaw Services, LTD, or to an international beneficiary.

84. BancorpSouth accepted the Wire Transfer for an amount greater than Choice's current ledger balance, despite Choice's wish, requirement and/or instruction that its account's current ledger balance govern whether or not BancorpSouth could accept a wire transfer, and despite Choice having never previously (i.e. with no frequency) transferring funds in an amount greater than Choice's current ledger balance.

85. BancorpSouth failed to adequately implement security procedures which effectively provided security against internet-based threats known on and prior to March 17, 2010.

86. There will likely be evidentiary support after a reasonable opportunity for further investigation or discovery that prior to March 17, 2010, BancorpSouth failed to adequately undertake, in a reasonable and timely manner, the risk assessments identified as a standard in the banking industry.

87. BancorpSouth failed to offer to Choice, or implement, security procedures which prevented foreign transfers.

88. BancorpSouth failed to offer to Choice, or implement, security procedures which utilized fraud-detection, behavioral analytics and/or fraud-monitoring.

89. BancorpSouth failed to emphasize to Choice the risks of internet banking, internet-based wire transfers, and the specific risks and liabilities associated with BancorpSouth's Dual Control and Single Control.

90. BancorpSouth failed to emphasize in its marketing efforts to obtain Choice as a customer, the nature of the risks associated with internet-based wire transfers, as opposed to focusing on and emphasizing the ease and efficiency of internet banking.

91. BancorpSouth failed to properly and adequately advise Choice of the proper safeguards and procedures to implement in order to protect Choice's InView account and security procedure information from internet-based threats.

92. BancorpSouth failed to recover any of the funds taken in the Wire Transfer after it received notice, and/or knew or should have known, that the Wire Transfer was not authorized by Choice.

93. BancorpSouth failed to initiate and maintain efforts in time to recover any of the funds taken in the Wire Transfer after it received notice, and/or knew or should have known, that the Wire Transfer was not authorized by Choice.

94. Choice exercised ordinary care in determining the Wire Transfer was not authorized by Choice and notified BancorpSouth that the Wire Transfer was unauthorized within a reasonable time, on March 18, 2010, the day after the Wire Transfer was accepted by BancorpSouth.

95. Pursuant to the facts described hereinabove, the Wire Transfer was not effective as an authorized payment order of Choice under Miss. Code Ann. §§75-4A-202(b) or (c), for any one or more of the following reasons:

a. the BancorpSouth security procedures offered and available to Choice on and before March 17, 2010, Single Control and Dual Control, were not commercially reasonable methods for providing security for Choice against unauthorized payment orders, considering Choice as the particular customer and BancorpSouth as the particular bank;

b. the BancorpSouth security procedures offered and available to Choice on and before March 17, 2010, were not commercially reasonable methods for providing security for Choice against unauthorized payment orders, since Single Control and Dual Control failed to meet prevailing standards of good banking practice applicable to BancorpSouth on and before March 17, 2010;

c. Single Control and Dual Control are not commercially reasonable or suitable or feasible for Choice, and Choice did not expressly agreed in writing to be bound by any payment order, whether or not authorized, issued in its name and accepted by BancorpSouth in compliance with Single Control;

d. Choice denies that BancorpSouth can prove it accepted the Wire Transfer in good faith;

e. Choice denies that BancorpSouth can prove it accepted the Wire Transfer in compliance with Choice's security procedure;

f. Choice denies that BancorpSouth can prove it accepted the Wire Transfer in compliance with the written agreements and/or instructions restricting acceptance of payment orders issued in Choice's name by and between Choice and BancorpSouth.

96. Pursuant to the facts described hereinabove, the Wire Transfer was not effective as an authorized payment order of Choice under Miss. Code Ann. §75-4A-202(a), in that:

a. The Wire Transfer was, in fact, not authorized by Choice, or its members, managers, agents, representatives, officers or employees;

b. The Wire Transfer was, in fact, not authorized by a person or entity with actual or apparent agency authority from Choice;

c. Choice did not, nor did a person or entity with actual or apparent agency authority from Choice, engage in conduct which would cause Choice to be bound by the unauthorized Wire Transfer or which would estop Choice from denying the Wire Transfer was authorized.

97. As a direct and proximate result of the foregoing, Choice suffered damages in the amount of $440,000.00, the full amount of the Wire Transfer that occurred on March 17, 2010, for which BancorpSouth is liable to Choice.

98. Pursuant to Miss. Code Ann. §§75-4A-204 and 75-4A-506, Choice is entitled to interest on its damages in the principal amount of $440,000.00, from the date the bank accepted the Wire Transfer (March 17, 2010) until the date of refund or repayment.

99. As a direct and proximate result of BancorpSouth's unauthorized acceptance of the Wire Transfer, Choice was required to retain attorneys in order to attempt to obtain refund or repayment of the funds that were transferred out of its account by BancorpSouth through the Wire Transfer, and Choice is thus entitled to its reasonable attorneys fees pursuant to the Court's equitable power to balance the benefits, since BancorpSouth is a large banking corporation and this is an unusual type of case or is unusually complicated litigation, in that it involves Article 4A of the Uniform Commercial Code (Miss. Code Ann. §§75-4A–101 et seq. (Rev. 2002)), which is rarely litigated, has little guiding or persuasive case law, and is an unusually complicated and technical area of the law.

100. Plaintiff Choice requests the Court enter Judgment as follows:

a. in Choice's favor and against Defendant BancorpSouth;

b. for damages in the principal amount of $440,000.00;

c. for interest on the principal amount of damages at the highest lawful interest rate, pursuant to Miss. Code Ann. §§75-4A–204 and 75-4A–506(b), from March 17, 2010 until the date of refund or repayment;

d. for its reasonable attorneys fees;

e. for the costs of this action;

f. for such other and further relief as to the Court seems just and proper.

WHEREFORE, Plaintiff Choice prays Judgment in its favor and against Defendant BancorpSouth; for damages in the principal amount of $440,000.00; for interest on the principal amount at the highest lawful interest rate, pursuant to Miss. Code Ann. §§75-4A–204 and 75-4A–506, from March 17, 2010 until the date of refund or repayment; for its reasonable attorney fees; for the costs of this action; and for such other and further relief as to the Court seems just and proper.

CHANEY & McCURRY

By /s/ Bruce McCurry
Bruce McCurry #22494

By /s/ Jeff McCurry
Jeff McCurry #61960

3249 E. Ridgeview Street
Springfield, MO 65804
417-887-4141 (Phone)
417-887-4177 (Fax)
bmccurry@bjklaw.com
jmccurry@bjklaw.com

Attorneys for Plaintiff Choice Escrow and Land Title, LLC

CERTIFICATE OF SERVICE

The undersigned, on behalf of Plaintiff, hereby certifies that the foregoing Second Amended Complaint was served by hand delivery and by electronic filling with the Clerk of the Court using the CM/ECF system, on August1, 2011, to:

Rodney Nichols
Carnahan, Evans, Cantwell & Brown, PC
2805 S. Ingram Mill Road
Springfield, Missouri, 65804

Attorneys for Defendant BancorpSouth Bank

/s/ Jeff McCurry

Jeff McCurry
Attorney for Plaintiff

Federal Financial Institutions Examination Council

Exhibit 1

3501 Fairfax Drive • Room 3086 • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 516-5487 • http://www.ffiec.gov

Authentication in an Internet Banking Environment

Purpose

On August 8, 2001, the FFIEC agencies[1] (agencies) issued guidance entitled *Authentication in an Electronic Banking Environment* (2001 Guidance). The 2001 Guidance focused on risk management controls necessary to authenticate the identity of retail and commercial customers accessing Internet-based financial services. Since 2001, there have been significant legal and technological changes with respect to the protection of customer information;[2] increasing incidents of fraud, including identity theft; and the introduction of improved authentication technologies. This updated guidance replaces the 2001 Guidance and specifically addresses why financial institutions regulated by the agencies should conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing their Internet-based financial services.

This guidance applies to both retail and commercial customers and does not endorse any particular technology. Financial institutions should use this guidance when evaluating and implementing authentication systems and practices whether they are provided internally or by a service provider. Although this guidance is focused on the risks and risk management techniques associated with the Internet delivery channel, the principles are applicable to all forms of electronic banking activities.

Summary of Key Points

The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Financial institutions offering Internet-based products and services to their customers should use effective methods to authenticate the identity of customers using those products and services. The authentication techniques employed by the financial institution should be appropriate to the risks associated with those products and services. Account fraud and identity theft are frequently the result of single-factor (e.g., ID/password) authentication exploitation. Where risk assessments indicate that the use of

---

[1] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

[2] Customer information means any record containing nonpublic personal information as defined in the Interagency Guidelines Establishing Information Security Standards at section I.C.2. 12 CFR Part 30, app. B (OCC); 12 CFR Part 208, app. D-2 and Part 225, app. F (FRB); 12 CFR Part 364, app. B (FDIC); 12 CFR Part 570, app. B (OTS); and 12 CFR Part 748, app. A (NCUA).

single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

Consistent with the *FFIEC Information Technology Examination Handbook*, Information Security Booklet, December 2002, financial institutions should periodically:

- Ensure that their information security program:
  - Identifies and assesses the risks associated with Internet-based products and services,
  - Identifies risk mitigation actions, including appropriate authentication strength, and
  - Measures and evaluates customer awareness efforts;

- Adjust, as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of its customer information, and internal or external threats to information; and

- Implement appropriate risk mitigation strategies.

Background

Financial institutions engaging in any form of Internet banking should have effective and reliable methods to authenticate customers. An effective authentication system is necessary for compliance with requirements to safeguard customer information,[3] to prevent money laundering and terrorist financing,[4] to reduce fraud, to inhibit identity theft, and to promote the legal enforceability of their electronic agreements and transactions. The risks of doing business with unauthorized or incorrectly identified persons in an Internet banking environment can result in financial loss and reputation damage through fraud, disclosure of customer information, corruption of data, or unenforceable agreements.

There are a variety of technologies and methodologies financial institutions can use to authenticate customers. These methods include the use of customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of "tokens", transaction profile scripts, biometric identification, and others. (The appendix to this guidance contains a more detailed discussion of authentication techniques.) The level of risk protection afforded by each of these techniques varies. The selection and use of authentication technologies and methods should depend upon the results of the financial institution's risk assessment process.

---

[3] The Interagency Guidelines Establishing Information Security Standards that implement section 501(b) of the Gramm–Leach–Bliley Act, 15 USC 6801, require banks and savings associations to safeguard the information of persons who obtain or have obtained a financial product or service to be used primarily for personal, family or household purposes, with whom the institution has a continuing relationship. Credit unions are subject to a similar rule.

[4] The regulations implementing section 326 of the USA PATRIOT Act, 31 USC § 5318(l), require banks, savings associations and credit unions to verify the identity of customers opening new accounts. See 31 CFR 103.121; 12 CFR 21.21 (OCC); 12 CFR 563.177 (OTS); 12 CFR 326.8 (FDIC); 12 CFR 208.63 (state member banks), 12 CFR 211.5(m) (Edge or agreement corporation or any branch or subsidiary thereof), 12 CFR 211.24(j) (uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States (FRB); and 12 CFR Part 748.2 (NCUA).

Existing authentication methodologies involve three basic "factors":

- Something the user ***knows*** (e.g., password, PIN);
- Something the user ***has*** (e.g., ATM card, smart card); and
- Something the user ***is*** (e.g., biometric characteristic, such as a fingerprint).

Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Accordingly, properly designed and implemented multifactor authentication methods are more reliable and stronger fraud deterrents. For example, the use of a logon ID/password is single-factor authentication (i.e., something the user knows); whereas, an ATM transaction requires multifactor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., PIN). A multifactor authentication methodology may also include "out–of–band"[5] controls for risk mitigation.

The success of a particular authentication method depends on more than the technology. It also depends on appropriate policies, procedures, and controls. An effective authentication method should have customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans.

Risk Assessment

The implementation of appropriate authentication methodologies should start with an assessment of the risk posed by the institution's Internet banking systems. The risk should be evaluated in light of the type of customer (e.g., retail or commercial); the customer transactional capabilities (e.g., bill payment, wire transfer, loan origination); the sensitivity of customer information being communicated to both the institution and the customer; the ease of using the communication method; and the volume of transactions. Prior agency guidance has elaborated on this risk-based and "layered" approach to information security.[6]

An effective authentication program should be implemented to ensure that controls and authentication tools are appropriate for all of the financial institution's Internet-based products and services. Authentication processes should be designed to maximize interoperability and should be consistent with the financial institution's overall strategy for Internet banking and electronic commerce customer services. The level of authentication used by a financial institution in a particular application should be appropriate to the level of risk in that application.

A comprehensive approach to authentication requires development of, and adherence to, the institution's information security standards, integration of authentication processes within the

---

[5] Out–of–band generally refers to additional steps or actions taken beyond the technology boundaries of a typical transaction. Callback (voice) verification, e-mail approval or notification, and cell–phone based challenge/ response processes are some examples.

[6] *FFIEC Information Technology Examination Handbook*, Information Security Booklet, December 2002; *FFIEC Information Technology Examination Handbook*, E-Banking Booklet, August 2003.

overall information security framework, risk assessments within lines of businesses supporting selection of authentication tools, and central authority for oversight and risk monitoring. This authentication process should be consistent with and support the financial institution's overall security and risk management programs.

The method of authentication used in a specific Internet application should be appropriate and reasonable, from a business perspective, in light of the reasonably foreseeable risks in that application. Because the standards for implementing a commercially reasonable system may change over time as technology and other procedures develop, financial institutions and technology service providers should develop an ongoing process to review authentication technology and ensure appropriate changes are implemented.

The agencies consider single-factor authentication, as the only control mechanism, to be inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. Single-factor authentication tools, including passwords and PINs, have been widely used for a variety of Internet banking and electronic commerce activities, including account inquiry, bill payment, and account aggregation. However, financial institutions should assess the adequacy of such authentication techniques in light of new or changing risks such as phishing, pharming,[7] malware,[8] and the evolving sophistication of compromise techniques. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks.

The risk assessment process should:

- Identify all transactions and levels of access associated with Internet-based customer products and services;

- Identify and assess the risk mitigation techniques, including authentication methodologies, employed for each transaction type and level of access; and

- Include the ability to gauge the effectiveness of risk mitigation techniques for current and changing risk factors for each transaction type and level of access.

Account Origination and Customer Verification

With the growth in electronic banking and commerce, financial institutions should use reliable methods of originating new customer accounts online. Moreover, customer identity verification during account origination is required by section 326 of the USA PATRIOT Act and is important in reducing the risk of identity theft, fraudulent account applications, and unenforceable account agreements or transactions. Potentially significant risks arise when a financial institution accepts new customers through the Internet or other electronic channels

[7] Similar in nature to e-mail phishing, pharming seeks to obtain personal information by directing users to spoofed Web sites where their information is captured, usually from a legitimate-looking form.
[8] Short for *malicious software,* such as software designed to capture and forward private information such as ID's, passwords, account numbers, and PINs.

because of the absence of the physical cues that financial institutions traditionally use to identify persons.

One method to verify a customer's identity is a physical presentation of a proof of identity credential such as a driver's license. Similarly, to establish the validity of a business and the authority of persons to perform transactions on its behalf, financial institutions typically review articles of incorporation, business credit reports, board resolutions identifying officers and authorized signers, and other business credentials. However, in an Internet banking environment, reliance on these traditional forms of paper-based verification decreases substantially. Accordingly, financial institutions need to use reliable alternative methods. (The appendix to this guidance describes verification processes in more detail.)

Monitoring and Reporting

Monitoring systems can determine if unauthorized access to computer systems and customer accounts has occurred. A sound authentication system should include audit features that can assist in the detection of fraud, money laundering, compromised passwords, or other unauthorized activities. The activation and maintenance of audit logs can help institutions to identify unauthorized activities, detect intrusions, reconstruct events, and promote employee and user accountability. In addition, financial institutions should report suspicious activities to appropriate regulatory and law enforcement agencies as required by the Bank Secrecy Act.[9]

Financial institutions should rely on multiple layers of control to prevent fraud and safeguard customer information. Much of this control is not based directly upon authentication. For example, a financial institution can analyze the activities of its customers to identify suspicious patterns. Financial institutions also can rely on other control methods, such as establishing transaction dollar limits that require manual intervention to exceed a preset limit.

Adequate reporting mechanisms are needed to promptly inform security administrators when users are no longer authorized to access a particular system and to permit the timely removal or suspension of user account access. Furthermore, if critical systems or processes are outsourced to third parties, management should ensure that the appropriate logging and monitoring procedures are in place and that suspected unauthorized activities are communicated to the institution in a timely manner. An independent party (e.g., internal or external auditor) should review activity reports documenting the security administrators' actions to provide the necessary checks and balances for managing system security.

Customer Awareness

Financial institutions have made, and should continue to make, efforts to educate their customers. Because customer awareness is a key defense against fraud and identity theft,

---

[9] 31 USC 5318; 12 CFR 21.11 (OCC); 12 CFR 563.180 (OTS); 12 CFR 353 (FDIC); 12 CFR 208.62 [state member banks]; 12 CFR 211.5 (k) [edge or agreement corporation, or any branch or subsidiary thereof]; 12 CFR 211.24 (f) [uninsured branch, an agency, or a representative office of a foreign financial institution operating in the United States]; 12 CFR 225.4 (f) [bank holding company or any non bank subsidiary thereof] (FRB); and 12 CFR Part 748.1 and Part 748.2 (NCUA).

financial institutions should evaluate their consumer education efforts to determine if additional steps are necessary. Management should implement a customer awareness program and periodically evaluate its effectiveness. Methods to evaluate a program's effectiveness include tracking the number of customers who report fraudulent attempts to obtain their authentication credentials (e.g., ID/password), the number of clicks on information security links on Web sites, the number of statement stuffers or other direct mail communications, the dollar amount of losses relating to identity theft, etc.

Conclusion

Financial institutions offering Internet-based products and services should have reliable and secure methods to authenticate their customers. The level of authentication used by the financial institution should be appropriate to the risks associated with those products and services. Financial institutions should conduct a risk assessment to identify the types and levels of risk associated with their Internet banking applications. Where risk assessments indicate that the use of single-factor authentication is inadequate, financial institutions should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate those risks. The agencies consider single-factor authentication, as the only control mechanism, to be inadequate in the case of high-risk transactions involving access to customer information or the movement of funds to other parties.

Appendix[10]

Background

The term *authentication*, as used in this guidance, describes the process of verifying the identity of a person or entity. Within the realm of electronic banking systems, the authentication process is one method used to control access to customer accounts and personal information. Authentication is typically dependent upon customers providing valid identification data followed by one or more authentication credentials (factors) to prove their identity.

Customer identifiers may be a bankcard for ATM usage, or some form of user ID for remote access. An authentication factor (e.g. PIN or password) is secret or unique information linked to a specific customer identifier that is used to verify that identity.

Generally, the way to authenticate customers is to have them present some sort of factor to prove their identity. Authentication factors include one or more of the following:

- *Something a person knows*—commonly a password or PIN. If the user types in the correct password or PIN, access is granted.
- *Something a person has*—most commonly a physical device referred to as a token. Tokens include self-contained devices that must be physically connected to a computer or devices that have a small screen where a one-time password (OTP) is displayed, which the user must enter to be authenticated.
- *Something a person is*—most commonly a physical characteristic, such as a fingerprint, voice pattern, hand geometry, or the pattern of veins in the user's eye. This type of authentication is referred to as "biometrics" and often requires the installation of specific hardware on the system to be accessed.

Authentication methodologies are numerous and range from simple to complex. The level of security provided varies based upon both the technique used and the manner in which it is deployed. Single-factor authentication involves the use of one factor to verify customer identity. The most common single-factor method is the use of a password. Two-factor authentication is most widely used with ATMs. To withdraw money from an ATM, the customer must present both an ATM card (*something the person has*) and a password or PIN (*something the person knows*). Multifactor authentication utilizes two or more factors to verify customer identity. Authentication methodologies based upon multiple factors can be more difficult to compromise and should be considered for high-risk situations. The effectiveness of a particular authentication technique is dependent upon the integrity of the selected product or process and the manner in which it is implemented and managed.

---

[10] This Appendix is based upon the FDIC Study – "Putting an End to Account-Hijacking Identity Theft" (December 14, 2004) and the FDIC Study Supplement (June 17, 2005).

Authentication Techniques, Processes, and Methodologies

Material provided in the following sections is for informational purposes only. The selection and use of any technique should be based upon the assessed risk associated with a particular electronic banking product or service.

Shared Secrets

Shared secrets (*something a person knows*) are information elements that are known or shared by both the customer and the authenticating entity. Passwords and PINs are the best known shared secret techniques but some new and different types are now being used as well. Some additional examples are:

- Questions or queries that require specific customer knowledge to answer, e.g., the exact amount of the customer's monthly mortgage payment.
- Customer-selected images that must be identified or selected from a pool of images.

The customer's selection of a shared secret normally occurs during the initial enrollment process or via an offline ancillary process. Passwords or PIN values can be chosen, questions can be chosen and responses provided, and images may be uploaded or selected.

The security of shared secret processes can be enhanced with the requirement for periodic change. Shared secrets that never change are described as "static" and the risk of compromise increases over time. The use of multiple shared secrets also provides increased security because more than onè secret must be known to authenticate.

Shared secrets can also be used to authenticate the institution's Web site to the customer. This is discussed in the Mutual Authentication section.

Tokens

Tokens are physical devices (*something the person has)* and may be part of a multifactor authentication scheme. Three types of tokens are discussed here: the USB token device, the smart card, and the password-generating token.

<u>USB Token Device</u>

The USB token device is typically the size of a house key. It plugs directly into a computer's USB port and therefore does not require the installation of any special hardware on the user's computer. Once the USB token is recognized, the customer is prompted to enter his or her password (the second authenticating factor) in order to gain access to the computer system.

USB tokens are one-piece, injection-molded devices. USB tokens are hard to duplicate and are tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials. The device has the ability to store digital certificates that can be used in a public key infrastructure (PKI) environment.

The USB token is generally considered to be user-friendly. Its small size makes it easy for the user to carry and, as noted above, it plugs into an existing USB port; thus the need for additional hardware is eliminated.

Smart Card

A smart card is the size of a credit card and contains a microprocessor that enables it to store and process data. Inclusion of the microprocessor enables software developers to use more robust authentication schemes. To be used, a smart card must be inserted into a compatible reader attached to the customer's computer. If the smart card is recognized as valid (first factor), the customer is prompted to enter his or her password (second factor) to complete the authentication process.

Smart cards are hard to duplicate and are tamper resistant; thus, they are a relatively secure vehicle for storing sensitive data and credentials. Smart cards are easy to carry and easy to use. Their primary disadvantage as a consumer authentication device is that they require the installation of a hardware reader and associated software drivers on the consumer's home computer.

Password-Generating Token

A password-generating token produces a unique pass-code, also known as a one-time password each time it is used. The token ensures that the same OTP is not used consecutively. The OTP is displayed on a small screen on the token. The customer first enters his or her user name and regular password (first factor), followed by the OTP generated by the token (second factor). The customer is authenticated if (1) the regular password matches and (2) the OTP generated by the token matches the password on the authentication server. A new OTP is typically generated every 60 seconds—in some systems, every 30 seconds. This very brief period is the life span of that password. OTP tokens generally last 4 to 5 years before they need to be replaced.

Password-generating tokens are secure because of the time-sensitive, synchronized nature of the authentication. The randomness, unpredictability, and uniqueness of the OTPs substantially increase the difficulty of a cyber thief capturing and using OTPs gained from keyboard logging.

Biometrics

Biometric technologies identify or authenticate the identity of a living person on the basis of a physiological or physical characteristic (*something a person is*). Physiological characteristics include fingerprints, iris configuration, and facial structure. Physical characteristics include, for example, the rate and flow of movements, such as the pattern of data entry on a computer keyboard. The process of introducing people into a biometrics-based system is called "enrollment." In enrollment, samples of data are taken from one or more physiological or physical characteristics; the samples are converted into a mathematical model, or template; and the template is registered into a database on which a software application can perform analysis.

Once enrolled, customers interact with the live-scan process of the biometrics technology. The live scan is used to identify and authenticate the customer. The results of a live scan, such as a fingerprint, are compared with the registered templates stored in the system. If there is a match, the customer is authenticated and granted access.

Biometric identifiers are most commonly used as part of a multifactor authentication system, combined with a password (*something a person knows*) or a token (*something a person has*).

Various biometric techniques and identifiers are being developed and tested, these include:

- fingerprint recognition;
- face recognition;
- voice recognition;
- keystroke recognition;
- handwriting recognition;
- finger and hand geometry;
- retinal scan; and
- iris scan.

Two biometric techniques that are increasingly gaining acceptance are fingerprint recognition and face recognition.

<u>Fingerprint Recognition</u>

Fingerprint recognition technologies analyze global pattern schemata on the fingerprint, along with small unique marks known as minutiae, which are the ridge endings and bifurcations or branches in the fingerprint ridges. The data extracted from fingerprints are extremely dense and the density explains why fingerprints are a very reliable means of identification. Fingerprint recognition systems store only data describing the exact fingerprint minutiae; images of actual fingerprints are not retained. Fingerprint scanners may be built into computer keyboards or pointing devices (mice), or may be stand-alone scanning devices attached to a computer.

Fingerprints are unique and complex enough to provide a robust template for authentication. Using multiple fingerprints from the same individual affords a greater degree of accuracy. Fingerprint identification technologies are among the most mature and accurate of the various biometric methods of identification.[11]

Although end users should have little trouble using a fingerprint-scanning device, special hardware and software must be installed on the user's computer. Fingerprint recognition implementation will vary according to the vendor and the degree of sophistication required. This technology is not portable since a scanning device needs to be installed on each participating user's computer. However, fingerprint biometrics is generally considered easier

[11] Currently, some financial institutions, domestic and foreign, that use fingerprint recognition and other biometric technologies to authenticate ATM users, are eliminating the need for an ATM card and the expense of replacing lost or stolen cards.

to install and use than other, more complex technologies, such as iris scanning. Enrollment can be performed either at the financial institution's customer service center or remotely by the customer after he or she has received setup instructions and passwords. According to fingerprint technology vendors, there are several scenarios for remote enrollment that provide adequate security, but for large-dollar transaction accounts, the institution should consider requiring that customers appear in person.

Face Recognition

Most face recognition systems focus on specific features on the face and make a two-dimensional map of the face. Newer systems make three-dimensional maps. The systems capture facial images from video cameras and generate templates that are stored and used for comparisons. Face recognition is a fairly young technology compared with other biometrics like fingerprints.

Facial scans are only as good as the environment in which they are collected. The so-called "mug shot" environment is ideal. The best scans are produced under controlled conditions with proper lighting and proper placement of the video device. As part of a highly sensitive security environment, there may be several cameras collecting image data from different angles, producing a more exact scan. Certain facial scanning applications also include tests for liveness, such as blinking eyes. Testing for liveness reduces the chance that the person requesting access is using a photograph of an authorized individual.

Non-Hardware-Based One-Time-Password Scratch Card

Scratch cards (*something a person has*) are less-expensive, "low-tech" versions of the OTP generating tokens discussed previously. The card, similar to a bingo card or map location look-up, usually contains numbers and letters arranged in a row-and-column format, i.e., a grid. The size of the card determines the number of cells in the grid.

Used in a multifactor authentication process, the customer first enters his or her user name and password in the established manner. Assuming the information is input correctly, the customer will then be asked to input, as a second authentication factor, the characters contained in a randomly chosen cell in the grid. The customer will respond by typing in the data contained in the grid cell element that corresponds to the challenge coordinates.

Conventional OTP hardware tokens rely on electronics that can fail through physical abuse or defects, but placing the grid on a wallet-sized plastic card makes it durable and easy to carry. This type of authentication requires no training and, if the card is lost, replacement is relatively easy and inexpensive.

Out-of-Band Authentication

Out-of-band authentication includes any technique that allows the identity of the individual originating a transaction to be verified through a channel different from the one the customer is using to initiate the transaction. This type of layered authentication has been used in the commercial banking/brokerage business for many years. For example, funds transfer requests,

purchase authorizations, or other monetary transactions are sent to the financial institution by the customer either by telephone or by fax. After the institution receives the request, a telephone call is usually made to another party within the company (if a business-generated transaction) or back to the originating individual. The telephoned party is asked for a predetermined word, phrase, or number that verifies that the transaction was legitimate and confirms the dollar amount. This layering approach precludes unauthorized transactions and identifies dollar amount errors, such as when a $1,000.00 order was intended but the decimal point was misplaced and the amount came back as $100,000.00.

In today's environment, the methods of origination and authentication are more varied. For example, when a customer initiates an online transaction, a computer or network-based server can generate a telephone call, an e-mail, or a text message. When the proper response (a verbal confirmation or an accepted-transaction affirmation) is received, the transaction is consummated.

Internet Protocol Address (IPA) Location and Geo-Location

One technique to filter an online transaction is to know who is assigned to the requesting Internet Protocol Address. Each computer on the Internet has an IPA, which is assigned either by an Internet Service Provider or as part of the user's network. If all users were issued a unique IPA that was constantly maintained on an official register, authentication by IPA would simply be a matter of collecting IPAs and cross-referencing them to their owners. However, IPAs are not owned, may change frequently, and in some cases can be "spoofed." Additionally, there is no single source for associating an IPA with its current owner, and in some cases matching the two may be impossible.

Some vendors have begun offering software products that identify several data elements, including location, anonymous proxies, domain name, and other identifying attributes referred to as "IP Intelligence." The software analyzes this information in a real-time environment and checks it against multiple data sources and profiles to prevent unauthorized access. If the user's IPA and the profiled characteristics of past sessions match information stored for identification purposes, the user is authenticated. In some instances the software will detect out-of-character details of the access attempt and quickly conclude that the user should not be authenticated.

Geo-location technology is another technique to limit Internet users by determining where they are or, conversely, where they are not. Geo-location software inspects and analyzes the small bits of time required for Internet communications to move through the network. These electronic travel times are converted into cyberspace distances. After these cyberspace distances have been determined for a user, they are compared with cyberspace distances for known locations. If the comparison is considered reasonable, the user's location can be authenticated. If the distance is considered unreasonable or for some reason is not calculable, the user will not be authenticated.

IPA verification or geo-location may prove beneficial as one factor in a multifactor authentication strategy. However, since geo-location software currently produces usable

results only for land-based or wired communications, it may not be suitable for some wireless networks that can also access the Internet such as cellular/digital telephones.

Mutual Authentication

Mutual authentication is a process whereby customer identity is authenticated and the target Web site is authenticated to the customer. Currently, most financial institutions do not authenticate their Web sites to the customer before collecting sensitive information. One reason phishing attacks are successful is that unsuspecting customers cannot determine they are being directed to spoofed Web sites during the collection stage of an attack. The spoofed sites are so well constructed that casual users cannot tell they are not legitimate. Financial institutions can aid customers in differentiating legitimate sites from spoofed sites by authenticating their Web site to the customer.

Techniques for authenticating a Web site are varied. The use of digital certificates coupled with encrypted communications (e.g. Secure Socket Layer, or SSL) is one; the use of shared secrets such as digital images is another. Digital certificate authentication is generally considered one of the stronger authentication technologies, and mutual authentication provides a defense against phishing and similar attacks.

Customer Verification Techniques

Customer verification is a related but separate process from that of authentication. Customer verification complements the authentication process and should occur during account origination. Verification of personal information may be achieved in three ways:

- *Positive verification* to ensure that material information provided by an applicant matches information available from trusted third party sources. More specifically, a financial institution can verify a potential customer's identity by comparing the applicant's answers to a series of detailed questions against information in a trusted database (e.g., a reliable credit report) to see if the information supplied by the applicant matches information in the database. As the questions become more specific and detailed, correct answers provide the financial institution with an increasing level of confidence that the applicant is who they say they are.

- *Logical verification* to ensure that information provided is logically consistent (e.g., do the telephone area code, ZIP code, and street address match).

- *Negative verification* to ensure that information provided has not previously been associated with fraudulent activity. For example, applicant information can be compared against fraud databases to determine whether any of the information is associated with known incidents of fraudulent behavior. In the case of commercial customers, however, the sole reliance on online electronic database comparison techniques is not adequate since certain documents (e.g., bylaws) needed to establish an individual's right to act on a company's behalf are not available from databases. Institutions still must rely on traditional forms of personal identification and document validation combined with electronic verification tools.

Another authentication method consists of the financial institution relying on a third party to verify the identity of the applicant. The third party would issue the applicant an electronic credential, such as a digital certificate, that can be used by the applicant to prove his/her identity. The financial institution is responsible for ensuring that the third party uses the same level of authentication that the financial institution would use itself.

Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation
National Credit Union Administration
Office of the Comptroller of the Currency
Office of Thrift Supervision

Frequently Asked Questions on

FFIEC Guidance on Authentication in an Internet Banking Environment

August 15, 2006

Purpose

The staffs of the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision (the Agencies) have jointly developed the attached frequently asked questions (FAQs) to assist financial institutions and their technology service providers in understanding the Federal Financial Institutions Examination Council's (FFIEC's) guidance entitled *Authentication in an Internet Banking Environment* (the guidance).

Overview

The guidance, issued on October 12, 2005, updates the FFIEC's guidance entitled *Authentication in an Electronic Banking Environment* issued in 2001. It addresses the need for risk based assessments, customer awareness, and enhanced security measures to authenticate customers using Internet-based products and services that process high risk transactions involving access to customer information or the movement of funds to other parties. The attached FAQs are a representation of questions the Agencies have received from financial institutions, Agency examiners, and technology service providers and they address the scope of the guidance, risk assessments, the time frame for implementation, and other issues.

Institutions should review these FAQs in conjunction with the guidance as they assess risks in their Internet-based products and services and determine appropriate authentication solutions for permitting access to systems that process high risk transactions involving the movement of funds to other parties or access to customer information.

Exhibit 2

Frequently Asked Questions on

FFIEC Guidance on Authentication in an Internet Banking Environment

Scope

Q-1- What was the impetus for the regulators providing guidance regarding how customers should access electronic banking systems?

A-1- Since 2001 there have been improvements in authentication technologies, increasing incidents of fraud (including identity theft), and significant legal and technological changes regarding the protection of customer information.

Q-2- Does the guidance apply to telephone banking systems?

A-2- While the guidance focuses on Internet banking systems, its principles apply to all forms of electronic banking, including telephone banking systems.

Q-3- Do the Agencies maintain a list of "approved" solutions?

A-3- No, the Agencies do not maintain a list of approved solutions.

Q-4- Is the Appendix to the guidance an "exclusive" list of solutions?

A-4- No, the Appendix is only a brief discussion of some of the technologies that the Agencies were aware of that could be used to address this issue.

Q-5- Does the guidance require the use of multifactor authentication?

A-5 No, the guidance does not call for the use of multifactor authentication. The use of multifactor authentication is one of several methods that can be used to mitigate risk as discussed in the guidance. However, the guidance identifies circumstances under which the Agencies would view the use of single-factor authentication as the only control mechanism as inadequate and conclude that additional risk mitigation is warranted.

Q-6- Does the guidance apply to both retail and commercial customers?

A-6- Yes, the guidance applies to both retail and commercial customers.

Q-7- Does the guidance apply to the retail use of credit and debit cards, including over the Internet?

A-7- No, the guidance does not apply to the use of credit or debit cards.

Q-8- Does the guidance apply to correspondent banking?

A-8- The guidance applies to correspondent banking if the correspondent banking relationship uses an electronic banking system with high-risk functionality as described in the guidance.

Q-9- Does the guidance specify the use of hardware tokens for authentication?

A-9 No, the use of hardware tokens is one possible method for enhancing controls surrounding the authentication of customers.

Q-10- Are the Agencies recommending multifactor authentication over layered security or other compensating controls?

A-10- No, any of these controls may be an effective method to mitigate risk in accordance with the guidance, if properly implemented.

Q-11- Are there banking applications where single-factor authentication as the only control mechanism would be adequate?

A-11- Single-factor authentication alone would be adequate for electronic banking applications that do not process high-risk transactions, e.g., systems that do not allow funds to be transferred to other parties or that do not permit access to customer information.

Q-12- Does the guidance apply to loan service companies?

A-12- The guidance applies to all financial institutions regulated by the Agencies.

Q-13- Does the guidance apply to securities brokers?

A-13- The guidance applies to the same entities and information covered by the Interagency Guidelines Establishing Information Security Standards. See ¶1.A of the Guidelines. The Securities and Exchange Commission has its own regulation on safeguarding customer information. See 17 C.F.R. 248.30.

Q-14- Can an institution perform a risk assessment and conclude that stronger authentication is not warranted?

A-14- An institution's risk assessment may conclude that existing controls are appropriate. However, such a conclusion would not be justified if the institution's electronic banking systems use single-factor authentication as their only control for high-risk transactions involving access to customer information or the movement of funds to other parties.

Q-15- If a financial institution has not experienced financial fraud or identity theft originating from its online banking system, should it nonetheless undertake risk mitigation steps in accordance with the guidance?

A-15- Yes, the guidance states that a financial institution's risk assessment should consider appropriate risk-mitigation steps for both current and future risks. (Please refer to question 14.)

Q-16- Does the guidance apply to loan or deposit account applications submitted over the Internet by non-customers?

A-16- The guidance does not apply to applications submitted by non-customers. As the appendix to the guidance explains, customer verification during account origination is a related but separate process from that of authentication.

Q-17- Does the guidance address mutual (e.g., institution-to-customer) authentication?

A-17- No, the guidance does not specifically address mutual authentication. However, mutual authentication may be an effective host authentication control mechanism and may be part of a layered security program.

Q-18- Would an institution meet the expectations of the guidance if it permits high-risk transactions through a system that relies on single-factor authentication as its only control mechanism provided that the institution chooses to reimburse customers for any losses associated with Internet fraud?

A-18- No, making customers whole for losses is not a substitute for adopting appropriate authentication measures or other controls described in the guidance.

Q-19- Does the guidance apply to call centers?

A-19- The principles of the guidance apply if a financial institution permits high-risk services to be performed through its call center.

Timing

Q-1- What do the Agencies expect institutions to have accomplished by year-end 2006?

A-1- The Agencies expect that institutions will complete the risk assessment and will implement risk mitigation activities by year-end 2006. The Agencies are not considering any general extension of the timing associated with this guidance.

Q-2- What if the financial institution or its technology service provider cannot implement a solution by year-end 2006?

A-2- The Agencies' examiners will assess the adequacy of each financial institution's authentication controls on a case-by-case basis.

Definitions

Q-1- Can you further clarify high-risk transactions involving the movement of funds to other parties and access to customer information?

A-1- The term "customer information" is defined in footnote 2 of the guidance by reference to the Interagency Guidelines Establishing Information Security Standards. Financial institutions may also want to review the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. The term "movement of funds to other parties" includes bill payment applications as well as the ability to transfer funds to a separate account maintained at the same depository institution but owned by a different party. Thus, any system that permits the movement of funds to other parties and/or the access to customer information, as defined previously, is "high-risk" necessitating stronger authentication or additional controls.

Q-2- What does the guidance mean when it refers to "layered security or other controls reasonably calculated to mitigate those risks?"

A-2 The term "layered security" includes other risk-mitigating controls that would not strictly be considered multifactor authentication. The reference to "other controls" includes other mitigating controls that exist today or that may be introduced in the future.

Risk Assessment

Q-1- What type of documentation is contemplated for the risk assessment? Do the Agencies have a template that financial institutions should use?

A-1- The guidance is not specific in this regard and the Agencies do not have a template for such risk assessments. However, financial institutions seeking general information on risk assessments may refer to the Small Entity Compliance Guide for the Interagency Guidelines Establishing Information Security Standards and the FFIEC IT Examination Handbook, Information Security Booklet.

Q-2- Can a financial institution rely on its Internet banking system provider to perform the risk assessment?

A-2- Yes, however, the institution is ultimately responsible for managing risk and should perform appropriate due diligence as required when selecting a service provider. The institution may accept a risk assessment performed by the service provider after the institution has ensured that the assessment is accurate and the solutions are sufficient to mitigate the risks to the financial institution and its customers.

Q-3- Does the guidance provide that financial institutions will assess the risks regarding authentication on a yearly basis?

A-3 No, however the Interagency Guidelines Establishing Information Security Standards require that an institution's information security program be monitored, evaluated, and adjusted as appropriate in light of changes in technology, the sensitivity of customer information, internal and external threats to information, the institution's changing business arrangements, and changes to customer information systems. These same criteria apply to re-evaluating the institution's Internet banking controls.

Q-4- Can a financial institution forgo the risk assessment and move immediately to implement additional authentication controls?

A-4- No, because the guidance is risk-based, a risk assessment that sufficiently evaluates the risks and identifies the reasons for choosing a particular control should be completed.

Q-5- Should the risk assessment specifically consider the risks of phishing, pharming, and malware?

A-5- Yes, these are some of the vulnerabilities that are specifically mentioned in the guidance. Other factors appropriate for consideration in the risk assessment include reputation risk, harm to the customer, transaction risk, and other reasonably foreseeable threats.

Customers

Q-1- May an institution permit customers to "opt-out" of additional authentication controls?

A-1- No, the Agencies believe that permitting customers to opt-out is not an effective risk mitigation strategy and would undermine the effectiveness of the control. In addition, this would not address reputation risk to the institution. However, an institution may permit customers to choose between different authentication options provided the options offered are consistent with the guidance.

Q-2- The guidance also discusses a customer awareness program that includes periodic evaluations. How do the Agencies envision that this would be implemented?

A-2- An institution may implement a customer awareness program in a number of ways, including making information available on the institution's website, in statement stuffers or other direct mail communication, or at branch offices. The institution may track the number of times customers click on an information security hotlink or the amount of written material disseminated. The Agencies understand that institutions cannot force customers to access or read such information.

Technology Service Providers

Q-1- Will the Agencies assess the progress of technology service providers prior to year-end 2006?

A-1- The Agencies are assessing efforts being made by technology service providers to conform with the guidance as part of the ongoing interagency supervisory process.

Q-2- Should an institution rely on the authentication technique chosen by its service provider?

A-2- The institution remains ultimately responsible for the adequate authentication of transactions involving access to customer information or movement of funds to other parties. This responsibility includes ensuring that the authentication techniques chosen by its service providers are appropriate for the institution's services.

Appendix

Q-1- Would two-factor authentication include using two of the same type of factor (e.g., two different passwords) if they are used at different points in the applications?

A-1- By definition true multifactor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category at different points in the process may be part of a layered security or other compensating control approach, but it would not constitute multifactor authentication.

Q-2- Is a user logon ID considered one of the factors in multifactor authentication?

A-2- No, because user logon IDs are not secret.

Q-3- Are there authentication methods that an institution can implement without customer involvement?

A-3- An institution can implement authentication controls with varying degrees of customer involvement. Some solutions can be implemented with virtually no customer interaction while others require significantly more.

Exhibit 3

FDIC

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-32-2007
April 11, 2007

IDENTITY THEFT
FDIC's Supervisory Policy on Identity Theft

Summary: The FDIC has issued the attached "Supervisory Policy on Identity Theft." The policy describes the characteristics of identity theft. It also sets forth the FDIC's expectations that institutions under its supervision take steps to detect and prevent identity theft and mitigate its effects in order to protect consumers and help ensure institutions' safe and sound operations.

Distribution:
FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
Chief Information Security Officer

Related Topics:
- FFIEC Information Security Handbook, issued July 2006
- FIL-18-2006, Fair Credit Reporting Act - Revised Examination Procedures (See module 5), February 22, 2006
- FIL-103-2005, Authentication in an Internet Banking Environment, October 12, 2005
- FIL-66-2005, Guidance on Mitigating Risks From Spyware, issued July 22, 2005
- FIL-64-2005, Guidance on How Financial Institutions Can Protect Against Pharming Attacks issued July 18, 2005
- Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, April 1, 2005
- FIL-27-2004, Guidance on Safeguarding Customers Against E-Mail and Internet Related Fraud, issued March 12, 2004
- Interagency Informational Brochure on Phishing Scams, contained in FIL-113-2004, issued September 13, 2004

Attachment:
Supervisory Policy on Identity Theft

Contact:
Senior Policy Analyst Jeffrey Kopchik at (202) 898-3872 or JKopchik@fdic.gov, or Policy Analyst (Compliance) David Lafleur at (202) 898-6569 or dlafleur@fdic.gov

Note:
FDIC financial institution letters (FILs) may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2007/index.html.

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1102, Arlington, VA 22226 (1-877-275-3342 or 202-416-6940).

Highlights:

- Identity theft poses risks to consumers and the safe and sound operation of financial institutions.
- The FDIC has well-defined expectations of how institutions should detect and prevent ID theft and mitigate its effects.
- The attached policy lays out the FDIC's approach to addressing identity theft, and contains standards that institutions are expected to meet to protect customers' sensitive information and notify them of compromises in appropriate circumstances.
- The FDIC believes that consumer education has an important role to play in helping to prevent identity theft and will continue its consumer education efforts during 2007.

Financial Institution Letters

Supervisory Policy on Identity Theft

Identity theft is fraud committed or attempted by using the identifying information of another person without his or her authority. Identifying information may include such things as a Social Security number, account number, date of birth, driver's license number, passport number, biometric data and other unique electronic identification numbers or codes. As more financial transactions are done electronically and remotely, and as more sensitive information is stored in electronic form, the opportunities for identity theft have increased significantly. [1] This policy statement describes the characteristics of identity theft and emphasizes the FDIC's well-defined expectations that institutions under its supervision detect, prevent and mitigate the effects of identity theft in order to protect consumers and help ensure safe and sound operations.

Characteristics of Identity Theft

At this time, the majority of identity theft is committed using hard-copy identification or other documents obtained from the victim without his or her permission.[2] A smaller, but significant, amount of identity theft is committed electronically via phishing, spyware, hacking and computer viruses. [3] Financial institutions are among the most frequent targets of identity thieves [4] since they store sensitive information about their customers and hold customer funds in accounts that can be accessed remotely and transferred electronically.

Identity theft may harm consumers in several ways. First, an identity thief may gain access to existing accounts maintained by consumers and either transfer funds out of deposit accounts or incur charges to credit card accounts. Identity thieves may also open new accounts in the consumer's name, incur expenses, and then fail to pay. This is likely to prompt creditors to attempt to collect payment from the consumer for debts the consumer did not incur. In addition, inaccurate adverse information about the consumer's payment history may prevent the consumer from obtaining legitimate credit when he or she needs it. An identity theft victim can spend months or years attempting to correct errors in his or her credit record.

FDIC Response to Identity Theft

The FDIC's supervisory programs include many steps to address identity theft. The FDIC acts directly, often in conjunction with other Federal regulators, by promulgating standards that financial institutions are expected to meet to protect customers' sensitive information and accounts. The FDIC enforces these standards against the institutions under its supervision and encourages all financial institutions to educate their customers about steps they can take to reduce the chances of becoming an identity theft victim. The FDIC also sponsors and conducts a variety of consumer education efforts to make consumers more aware of the ways they can protect themselves from identity thieves.

Supervisory Action

As a result of guidelines issued by the FDIC, together with other federal agencies, financial institutions are required to develop and implement a

written program to safeguard customer information, including the proper disposal of consumer information (Security Guidelines).[5] The FDIC considers this programmatic requirement to be one of the foundations of identity theft prevention. In guidance that became effective on January 1, 2007, the federal banking agencies made it clear that they expect institutions to use stronger and more reliable methods to authenticate the identity of customers using electronic banking systems.[6] Moreover, the FDIC has also issued guidance stating that financial institutions are expected to notify customers of unauthorized access to sensitive customer information under certain circumstances.[7] The FDIC has issued a number of other supervisory guidance documents articulating its position and expectations concerning identity theft.[8] Industry compliance with these expectations will help to prevent and mitigate the effects of identity theft.

Risk management examiners trained in information technology (IT) and the requirements of the Bank Secrecy Act (BSA) evaluate a number of aspects of a bank's operations that raise identity theft issues. IT examiners are well-qualified to evaluate whether banks are incorporating emerging IT guidance into their Identity Theft Programs and GLBA 501(b) Information Security Programs; responsibly overseeing service provider arrangements; and taking action when a security breach occurs. In addition, IT examiners will consult with BSA examiners during the course of an examination to ensure that the procedures institutions employ to verify the identity of new customers are consistent with existing laws and regulations to prevent financial fraud, including identity theft.

The FDIC has also issued revised examination procedures for the Fair Credit Reporting Act (FCRA), through the auspices of the Federal Financial Institutions Examination Council's (FFIEC) Consumer Compliance Task Force. [9] These procedures are used during consumer compliance examinations and include steps to ensure that institutions comply with the FCRA's fraud and active duty alert provisions. These provisions enable consumers to place alerts on their consumer reports that require users, such as banks, to take additional steps to identify the consumer before new credit is extended. The procedures also include reviews of institutions' compliance with requirements governing the accuracy of data provided to consumer reporting agencies. These requirements include the blocking of data that may be the result of an identity theft. Compliance examiners are trained in the various requirements of the FCRA and ensure that institutions have effective programs to comply with the identity theft provisions. Consumers are protected from identity theft through the vigilant enforcement of all the examination programs, including Risk Management, Compliance, IT and BSA.

The Fair and Accurate Credit Transactions Act directed the FDIC and other federal agencies to jointly promulgate regulations and guidelines that focus on identity theft "red flags" and customer address discrepancies. As proposed, [10] the guidelines would require financial institutions and creditors to establish a program to identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft. The proposed joint regulation would require financial institutions and creditors to establish reasonable policies to implement the guidelines, including a provision requiring debit and credit card issuers to assess the validity of a request for a change of address. In addition, the agencies proposed joint regulations that provide guidance regarding reasonable policies and procedures that a user of consumer reports must employ when the user receives a notice of address discrepancy. When promulgated in final form, these joint regulations and guidelines will comprise another element of the FDIC's program to prevent and mitigate identity theft.

Consumer Education

The FDIC believes that consumers have an important role to play in protecting themselves from identity theft. As identity thieves become more sophisticated, consumers can benefit from accurate, up-to-date information designed to educate them concerning steps they should take to reduce their vulnerability to this type of fraud. The financial services industry, the FDIC

and other federal regulators have made significant efforts to raise consumers' awareness of this type of fraud and what they can do to protect themselves.

In 2005, the FDIC sponsored four identity theft symposia entitled *Fighting Back Against Phishing and Account-Hijacking.* At each symposium (held in Washington, D.C., Atlanta, Los Angeles and Chicago), panels of experts from government, the banking industry, consumer organizations and law enforcement discussed efforts to combat phishing and account hijacking, and to educate consumers on avoiding scams that can lead to account hijacking and other forms of identity theft. Also in 2006, the FDIC sponsored a symposia series entitled *Building Confidence in an E-Commerce World.* Sessions were held in San Francisco, Phoenix and Miami. Further consumer education efforts are planned for 2007.

In 2006, the FDIC released a multi-media educational tool, *Don't Be an On-line Victim*, to help online banking customers avoid common scams. It discusses how consumers can secure their computer, how they can protect themselves from electronic scams that can lead to identity theft, and what they can do if they become the victim of identity theft. The tool is being distributed through the FDIC's web site and via CD-ROM. Many financial institutions also now display anti-fraud tips for consumers in a prominent place on their public web site and send customers informational brochures discussing ways to avoid identity theft along with their account statements. Financial institutions are also redistributing excellent educational materials from the Federal Trade Commission, the federal government's lead agency for combating identity theft.

President's Identity Theft Task Force

On May 10, 2006, the President issued an executive order establishing an Identity Theft Task Force (Task Force). The Chairman of the FDIC is a principal member of the Task Force and the FDIC is an active participant in its work. The Task Force has been charged with delivering a coordinated strategic plan to further improve the effectiveness and efficiency of the federal government's activities in the areas of identity theft awareness, prevention, detection, and prosecution. On September 19, 2006, the Task Force adopted interim recommendations on measures that can be implemented immediately to help address the problem of identity theft. Among other things, these recommendations dealt with data breach guidance to federal agencies, alternative methods of "authenticating" identities, and reducing access of identity thieves to Social Security numbers. The final strategic plan is expected to be publicly released soon.

Conclusion

Financial institutions have an affirmative and continuing obligation to protect the privacy of customers' nonpublic personal information. Despite generally strong controls and practices by financial institutions, methods for stealing personal data and committing fraud with that data are continuously evolving. The FDIC treats the theft of personal financial information as a significant risk area due to its potential to impact the safety and soundness of an institution, harm consumers, and undermine confidence in the banking system and economy. The FDIC believes that its collaborative efforts with the industry, the public and its fellow regulators will significantly minimize threats to data security and consumers.

---

[1]See *Study on "Account-Hijacking" Identity Theft and Suggestions for Reducing Online Fraud*, FDIC FIL-132-2004, December 14, 2004; *Study Supplement on "Account-Hijacking" Identity Theft*, FDIC FIL-59-2005, July 5, 2005.
[2]*2006 Identity Fraud Survey Report*, Javelin Strategy & Research, January 2006.
[3]Ibid.
[4]ID Theft Resource Center, security breaches as of January 16, 2007, http://www.idtheftcenter.org/breaches.shtml.

[5]12 CFR 364, Appendix B [illegible] $250,000 per insured bank

[6]*Authentication in an Internet Banking Environment*, FDIC FIL-103-2005, October 12, 2005.

[7]*Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, FDIC FIL-27-2005, April 1, 2005.

[8]See *Guidance on Security Risks of VOIP*, FDIC FIL-69-2005, July 27, 2005; *Guidance on Mitigating Risks from Spyware*, FDIC FIL-66-2005, July 22, 2005; *How Financial Institutions Can Protect Against Pharming Attacks*, FDIC FIL-64-2005, July 18, 2005; *Interagency Informational Brochure on Internet "Phishing" Scams*, FDIC FIL-103-3004, September 13, 2004; *Identity Theft and Pretext Calling*, FDIC FIL-39-2001, May 9, 2001.

[9]*Fair Credit Reporting Act – Revised Examination Procedures*, FDIC FIL-18-2006, February 22, 2006.

[10]**See**, 71 Federal Register 40786, published on July 18, 2006.

Special Alerts

SA-147-2009
August 26, 2009

Exhibit 4

TO: CHIEF EXECUTIVE OFFICER
SUBJECT: Fraudulent Electronic Funds Transfers (EFTs)
Summary: *The Federal Deposit Insurance Corporation is aware of an increased number of fraudulent EFT transactions resulting from compromised login credentials.*

The Federal Deposit Insurance Corporation (FDIC) is alerting financial institutions that provide Web-based payment origination services for business customers to increased reports of fraudulent EFT transactions resulting from compromised login credentials. Over the past year, the FDIC has detected an increase in the number of reports and the amount of losses resulting from unauthorized EFTs, such as automated clearing house (ACH) and wire transfers. In most of these cases, the fraudulent transfers were made from business customers whose online business banking software credentials were compromised.

Web-based commercial EFT origination applications are being targeted by malicious software, including Trojan horse programs, key loggers and other spoofing techniques, designed to circumvent online authentication methods. Illicitly obtained credentials can be used to initiate fraudulent ACH transactions and wire transfers, and take over commercial accounts. These types of malicious code, or "crimeware," can infect business customers' computers when the customer is visiting a Web site or opening an e-mail attachment. Some types of crimeware are difficult to detect because of how they are installed and because they can lie dormant until the targeted online banking session login is initiated. These attacks could result in monetary losses to financial institutions and their business customers if not detected quickly.

Financial institutions and technology service providers can refer to the following guidance for additional information on authentication and information security for high-risk transactions:

FFIEC Guidance Authentication in an Internet Banking Environment
Authentication in an Internet Banking Environment Frequently Asked Questions
FFIEC Information Security Examination Handbook - PDF 866k (PDF Help)
FFIEC Retail Payment Systems Examination Handbook
and
FDIC Guidance on Mitigating Risks from Spyware

Consumers who want to learn more about computer security and online scams can find additional information at http://www.fdic.gov/consumers/consumer/guard/index.html and http://www.onguardonline.gov/topics/overview.aspx.

Businesses and local government agencies can find cyber security resources at http://www.us-cert.gov/.

Information about cyber-fraud incidents and other fraudulent activity may be forwarded to the FDIC's Cyber-Fraud and Financial Crimes Section, 550 17th Street, N.W., Room F-4004, Washington, D.C. 20429, or transmitted electronically to alert@fdic.gov. Questions related to federal deposit insurance or consumer issues should be submitted to the FDIC using an online form that can be accessed at http://www2.fdic.gov/starsmail/index.asp.

For your reference, FDIC Special Alerts may be accessed from the FDIC's website at www.fdic.gov/news/news/SpecialAlert/2009/index.html. To learn how to automatically receive FDIC Special Alerts through e-mail, please visit www.fdic.gov/about/subscriptions/index.html.

Sandra L. Thompson
Director
Division of Supervision and Consumer Protection

Distribution: FDIC-Supervised Banks (Commercial and Savings)

Outgoing Funds Transfer Advice
FACSIMILE TRANSACTION RECEIPT

This facsimile receipt serves as immediate notification of the following Fed Funds Transfer that will be DEBITED from account. If you have any questions, please contact your local branch.

Amount: $440,000.00

Account Number: #618003800

* * *

Sender ABA: 065300486 Sender Name: BancorpSouth

Sender Reference: 0866102

Receiver ABA: 021000018 Receiver Name: BANK OF NEW YORK

* * *

Beneficiary: BROLAW SERVICES LTD

Beneficiary Bank: POPULAR BANK PUBLIC CO LTD

* * *

Originator Info: Choice Escrow and Land Title LLC

Originator Bank: BancorpSouth

Originator Bank Info: Invoice:equipment

Bank to Bank Info: [6100]NEW YORK*NEW YORK*

FED IMAD Confirmation#:20100317F5QCZ68C000150

* * *

CHOICE ESCROW & LAND TITLE LLC
TRUST ACCOUNT
ESCROW DISBURSEMENT ACCT 1440 E PRIMROSE ST
SPRINGFIELD, MO 65804-4290

Exhibit 5

RECEIVED MAY 14 2009

COPY

BANCORPSOUTH BANK
FUNDS TRANSFER AGREEMENT

THIS FUNDS TRANSFER AGREEMENT is made and entered into on the date set forth below by and between Choice Escrow & Land Title LLC (hereinafter called "Customer") and BancorpSouth Bank, a Mississippi banking corporation, (hereinafter called "Bank").

IN CONSIDERATION of the mutual promises made herein and other good and valuable consideration, the full sufficiency of which is hereby acknowledged, the parties agree as follows:

I. Customer authorizes and requests Bank to make transfers of funds from time to time in accordance with the provisions and procedures more fully set forth in this Agreement. Such transfers shall include transfers of Customer's funds from Customer's account(s) at Bank, hereinafter called "Account(s)", to Customer's accounts at Bank or other depository institutions, and to account(s) of third parties at other depository institutions, and shall also include transfers of funds to Customer's Account(s) from third parties. Remittance may be made by Bank through any of its customary channels.

II. Requests from Customer to Bank shall be made by Customer's representatives ("Authorized Agents") listed on the Funds Transfer Authorization form furnished by Customer to Bank. Elimination or addition of any Authorized Agent shall be accomplished by Customer's submission to Bank of a new Funds Transfer Authorization form. Such elimination or addition shall not be effective until such new form is actually received by Bank. Customer accepts responsibility for informing its Authorized Agents of the terms of this Agreement and the procedures required hereunder.

III. Any Authorized Agent may request or authorize one or more funds transfers. Requests for funds transfers may be made by telephone, in person, by written instruction, or by any other means of communication acceptable to Bank subject to time deadlines established by Bank.

IV. Bank may make the requested funds transfer by any means for the transmission of funds and may also make transfers by internal means (including, but not limited to, its correspondent banks). Transfers of funds to Customer's Account(s) from third parties shall be received subject to time deadlines established by Bank. Bank may cancel a requested funds transfer if Bank receives Customer's request for cancellation in form satisfactory to Bank in such time and manner as to allow Bank reasonable opportunity to act.

V. In consideration of Bank's transfer of funds pursuant to Customer's authorized requests, Customer shall pay to Bank such transfer fees as Bank shall from time to time impose.

VI. Bank will use ordinary care in implementing funds transfers requests received by Bank from Customer. Customer agrees that Bank and its agents and correspondents shall be conclusively deemed to have exercised ordinary care if it or they has or have followed the procedures contained in this Agreement. Bank shall be entitled to rely on any request that it believes to have been originated by Customer, and any such request shall for purposes of this Agreement be deemed to have been authorized by Customer.

VII. Bank shall be responsible only for performing the services expressly provided for in this Agreement and shall be liable only for its failure to use ordinary care in performing those services. Bank shall not be responsible for Customer's acts, failures or omissions or those of any other person (including, but not limited to, Bank's vendors and suppliers, other depository institutions, and the Fedwire Federal Reserve funds transfer system). Customer agrees to indemnify Bank against any loss, liability or expense (including attorney's fees and expenses) resulting from or arising out of any claim of any person that Bank is responsible for any act or omission of Customer or any other person. Bank shall not be liable for failing to act or for delay in acting if such failure or delay is caused by legal constraint, interruption of transmission or communication facilities, equipment failure, war, emergency conditions or other circumstances beyond Bank's control. In addition, Bank shall be excused from failing to execute and from delay in executing a transfer if such transfer would result in Bank having exceeded any limitation upon its intra-day net funds position established pursuant to present or future Federal Reserve guidelines or in Bank's otherwise violating any provision of any present or future risk control program of the Federal Reserve or any rule or regulation of any other regulatory authority.

VIII. In order to authenticate funds transfer requests, Bank shall assign to Customer a security code which must be used by all Authorized Agents in making such requests. Bank will not accept any request hereunder without the valid security code. Customer accepts responsibility for advising its Authorized Agents of the security code, and Customer agrees that it and its Authorized Agents will safeguard the security code. Any request received by Bank with the valid security code shall be irrebuttably presumed to be from an Authorized Agent. Bank reserves the right to change the security code from time to time. In the event of the elimination of any Authorized Agent from Customer's Funds Transfer Authorization form, Bank shall assign a new security code, and Customer agrees not to request any further transfers until such new code has been assigned.

IX. Bank will furnish to Customer confirmed notification of a funds transfer after it is made, either in the form of a specific advice or a periodic account statement. Customer will examine such advice and account statements to detect the presence or absence of any discrepancies between Customer's records and the advice or statement sent by Bank, and will report any such discrepancies to Bank within thirty (30) days after the day that Bank sends the advice or account statement.

X. The amount of payment will be placed at the disposal of the correspondent bank under advice by telegraph, phone, cable or mail as the case may be, and Bank assumes no further responsibility for the availability of the credit or for the payment of the funds to the beneficiary, all of which risks are assumed by Customer. Bank shall be under no obligation to obtain the receipt of the beneficiary or otherwise verify payment.

XI. Bank is hereby authorized, but not required, to record on tape or other retention devices any and all of its conversations with Customer and Authorized Agents involving any matter relating to this agreement. (Notification under FCC #263)

XII. Customer agrees to supply to Bank information that Bank may reasonably request in connection with any prospective or completed funds transfer hereunder, including without limitation any writings showing confirmation of any request for transfer of funds.

XIII. Bank shall not be obligated to make any funds transfer if the amount of such transfer exceeds the finally collected and immediately available funds on deposit by Customer with Bank, or exceeds any other limit established by Bank. If Bank in its discretion makes any such transfer that exceeds the amount of Customer's deposited funds, Customer shall be liable for any and all overdraft amounts. Bank reserves the right to refuse any telephone request.

XIV. All data relative to Customer's business provided to Bank by Customer pursuant to this Agreement will be treated confidentially and safeguarded by Bank, using the same care and discretion that is used with data that Bank designates as confidential.

XV. Bank may modify or terminate this Agreement immediately upon providing written notice of such termination to Customer. Customer may terminate this Agreement upon fifteen (15) days written notice to Bank.

XVI. This Agreement supplements the separate Account Agreement(s) governing Customer's account(s) from which funds are transferred hereunder. In the event of any conflict between the terms of this Agreement and such Account Agreement(s), this Agreement controls. Otherwise, this Agreement comprises the complete and exclusive statement of the agreement between Bank and Customer with respect to the subject matter hereof and supersedes any prior agreements between Bank and Customer with respect to such subject matter. In the event performance of the services provided herein in accordance with the terms of this Agreement would result in a violation of any present or future statute, regulation or government policy to which Bank is subject and which governs or affects the transactions contemplated by this Agreement, then this Agreement shall be deemed amended to the extent necessary to comply with such statute, regulation or policy, and Bank shall incur no liability to Customer as a result of such violation or amendment. This Agreement is not for the benefit of any other person, and no other person shall have any right against Bank or Customer hereunder. This Agreement shall be construed in accordance with and governed by the laws of the State of Mississippi. Bank and Customer agree that the venue for any litigation arising in connection with this Agreement shall be Lee County, Mississippi.

XVII. Any notice hereunder (except those from Bank pursuant to Paragraph X) shall be sent via commercial overnight courier or certified first class mail with return receipt addressed as follows or as otherwise direct in writing by the other party. Any notice from Bank to Customer may, at Bank's discretion, be sent via telecopier.

Bank:
BancorpSouth Bank
Attn: Wire Transfer Department
Post Office Drawer 789
Tupelo, MS 38802-0789

Customer:
Choice Escrow & Land Title LLC
1440 E. Primrose
Springfield, MO 65804
Telecopier:

EXECUTED ON THIS THE 16 DAY OF April 2009.

CUSTOMER:

By: L. Paige Payne

Title: Member

BANK:

BANCORPSOUTH BANK

By:

Title: CSR

Exhibit 6

RECEIVED APR 23 2009

COPY

BANCORPSOUTH BANK
BUSINESS SERVICES AGREEMENT

THIS AGREEMENT made this 16th day of April, 2009, by and between BancorpSouth Bank, at and through its offices located at 3211 E Battlefield Springfield, MO 65804 (hereinafter "BancorpSouth"), and Choice Escrow and Land Title, LLC

☐ sole proprietorship ☐ partnership ☐ corporation ☒ other: LLC
with principal offices at 1440 E. Primrose Springfield, MO 65804
(hereinafter the "Customer").

BancorpSouth shall perform services described in separate Implementation Form(s) (hereinafter collectively the "Services"), in accordance with the terms and conditions of this Agreement and the respective Implementation Form(s). If the terms of the Form(s) conflict with the terms of this Agreement, the terms of the Form(s) shall apply.

1. **RELATED AGREEMENTS.** This Agreement shall be supplementary to, and be construed in conjunction with any and all other Account Agreement(s), ("Signature Cards"), Resolutions, Implementation Forms, Addendums, and other documents and agreements covering Customer's Account(s) with BancorpSouth. All such written agreements constitute the full and entire agreement regarding the Services. If the terms of this Agreement conflict with the terms of any other Account Agreement or Resolution associated therewith, the terms of such separate Account Agreement or Resolution shall control.

2. **SERVICES.** BancorpSouth shall perform Services in accordance with the terms and conditions of this Agreement and as more particularly described in separate Implementation Form(s). Implementation Form(s) shall constitute Customer's election as to specific Services offered hereunder and shall become effective as both parties hereto may execute one or more of same from time to time either contemporaneous herewith or hereafter; all of which shall constitute counterparts and exhibits to this Agreement. The Customer agrees that the Services to be performed by BancorpSouth will be used by the Customer solely for business or commercial purposes and not personal or consumer purposes.

3. **FEES.** The Customer shall pay for Services such fees in accordance with BancorpSouth's schedule of fees in effect from time to time (the "Fees"). A current schedule of Fees is available from BancorpSouth. Fees are also payable through the maintenance by Customer of compensating collected balances in specified account(s). The compensating collected balance requirement will be measured by BancorpSouth by profitability analysis of the Customer's specified account(s). Fees are payable monthly and BancorpSouth is authorized to charge the Fees on the due dates to specified

Customer account(s) or bill by monthly invoice, at its option. Fees, which are charged to a Customer's account, shall be reflected on Customer's monthly statement of account.

4. **CUSTOMER'S RECORDS AND MEDIA.** The Customer will provide BancorpSouth all records and data processing media necessary to perform the Services. The records will be legible, correct, complete and in the format specified on the Implementation Form(s). The records will contain all necessary information as determined by, and satisfactory to, BancorpSouth. All data processing media supplied by the Customer must be compatible with BancorpSouth systems and equipment. Checks will be MICR encoded according to BancorpSouth specifications.

   If this Agreement is terminated, the Customer will notify BancorpSouth in writing within 30 days of the effective date of termination whether BancorpSouth should return or destroy any data processing media furnished by the Customer and any records in its possession or produced as a result of the expiring Services. If the Customer does not notify BancorpSouth within 30 days, BancorpSouth may destroy, retain or return any such material, as Customer would have then been deemed to have abandoned such media; therefore all risk of loss is with Customer and BancorpSouth shall have no responsibility for said media, or liability to Customer for same, if the media is destroyed, not returned, or otherwise dealt with by BancorpSouth.

   All specifications, tapes or other media, and all programs and procedures utilized or developed by BancorpSouth in connection with the performance of the Services, are, will be and shall remain the sole property of BancorpSouth. In the event of termination of this Agreement, the Customer is responsible for their prompt return and shall return same, with any damages incurred in shipping and usage other than normal wear and tear being the sole responsibility of Customer.

5. **CUSTOMER'S FAILURE TO FURNISH SATISFACTORY RECORDS OR MEDIA.** BancorpSouth's performance is based on BancorpSouth receiving timely, accurate and complete data for each Service, acceptable to BancorpSouth, and which can be used on BancorpSouth systems or equipment. If any of these requirements are not met by the Customer, BancorpSouth shall:

   a. no longer be bound to the normal delivery schedule;
   b. be empowered to charge appropriate fees for the cost of converting nonstandard data into standard form, or complete missing data, in its discretion;
      and/or
   c. be authorized to deliver as complete and finished whatever portion of the Services can be performed with the data available.

6. **CUSTOMER'S DUTY TO INSPECT.** The Customer is responsible to inspect all Services performed when received and to notify BancorpSouth immediately of any errors. For daily Services, the Customer must give notice to BancorpSouth within a reasonable time after receipt of the material containing an error. The parties hereby mutually agree that a reasonable time to give notice to BancorpSouth shall be thirty (30)

days after receipt. Receipt shall mean actual delivery, if proof thereof is available to BancorpSouth; otherwise, receipt shall be deemed to have occurred three (3) banking days after the date of the material containing an error. A failure to give notice to BancorpSouth of error(s) within this time will relieve BancorpSouth of any and all liability.

7. **FACSIMILE SIGNATURE.** If the Customer at any time and in any manner, (including authorizations made by Account Agreement or Resolution), authorizes utilization of a facsimile signature, BancorpSouth shall be entitled to honor such facsimile signature for all purposes hereunder, including, but not limited to, charging Customer for such checks or other orders for payment of money so signed, regardless of by whom or what means the purported or actual facsimile signature may have been made or affixed thereto. Customer agrees and warrants that all previous and present authorizations are continued in full force and effect.

8. **LIMITATION OF LIABILITY.** It is understood that BancorpSouth will make reasonable best efforts to select and use facilities, equipment and personnel in connection with the Services to be performed under this Agreement so as to render error-free services. Otherwise, no warranties, express or implied, of any kind are offered or intended. BancorpSouth's sole responsibility for any error is to correct that error, provided BancorpSouth has received notice within a reasonable time, as specified in Section 6 hereof, for each Service. Correction of errors shall be Customer's sole and exclusive remedy. **BANCORPSOUTH HEREBY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, ARISING BY OPERATION OF LAW OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY AS TO MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.** Notwithstanding the foregoing, in the event BancorpSouth cannot correct an error, and solely in the event the Customer incurs a direct actual loss as a result thereof which is due to the negligence of BancorpSouth with respect to any entry or entries, BancorpSouth's maximum liability to the Customer shall be limited to (a) actual money damages not to exceed the actual money damages sustained and proven by the Customer, reduced on a comparative basis by the negligence, if any, of Customer, or (b) the total amount due from the Customer for the specific Services in connection with the uncorrected error(s) for the month during which those Services in connection with the uncorrected error(s) were performed, WHICHEVER IS LESS. In no event will BancorpSouth be liable or answerable to the Customer or any other party for any lost profits or any consequential, compensatory, punitive, special, or other damages caused by any error, act, delay or omission on BancorpSouth's part.

9. **INDEMNITY.** As long as BancorpSouth has performed as provided in Section 8 above, the Customer shall indemnify and hold BancorpSouth harmless from any and all claims, damages, losses, liabilities and cost or expenses, including reasonable attorneys' fees, which relate in any manner to the Services performed under this Agreement.

10. **TERMINATION.** This Agreement shall continue unless terminated (a) by either party upon thirty (30) days prior written notice to the other party, in which event

termination shall be deemed effective at the next statement cycle nearest to the expiration of the thirty (30) days notice of termination, as determined by BancorpSouth; (b) by BancorpSouth, if BancorpSouth determines in good faith that material just cause exists for terminating this Agreement (and in such event, BancorpSouth may terminate this Agreement at any time without notice to Customer); or (c) upon closing of any Account associated with the Services contemplated hereunder (and in such event, termination shall be immediate upon date of closure of such account).

11. **NOTICES.** Any notices and other communications required or permitted hereunder shall be in writing and shall be sent:

A. **To BancorpSouth at:**

ATTN: Treasury Management
(Department)

BancorpSouth Bank

3211 E. Battlefield
(Address)

Springfield, MO 65804
(City/State/Zip)

B. **To Customer at:**

ATTN: L. Paige Payne
(Name / Department)

Choice Escrow and Land Title, LLC
(Company)

1440 E. Primrose
(Address)

Springfield, MO 65804
(City/State/Zip)

Except as otherwise provided herein, notice shall be effective upon receipt.

12. **NON-PERFORMANCE/FORCE MAJEURE.** BancorpSouth shall bear no responsibility for non-performance of one or more Services caused by major events beyond its control, such as: fire, casualty, breakdown in equipment, lockout, strike, unavoidable accident, act of God, riot, war or the enactment, issuance or operation of any adverse governmental law, ruling regulation, order or decree, or emergency that prevents us from operating normally.

13. **MISCELLANEOUS.**

A. **Amendments.** This Agreement may not be amended except by mutual written agreement of the parties hereto.

B. **Governing Law.** This Agreement shall be governed by the laws of the State of location of the BancorpSouth branch identified in the Notice provision hereof, without regard to such state's conflicts of laws rules.

C. **Limitation and Assignment.** The parties acknowledge and agree that this agreement constitutes a contract to extend financial accommodations solely to and for the benefit of Customer. No third party beneficiary rights exist hereunder, nor are same intended. Customer rights and duties hereunder may not be assigned without the prior written consent of BancorpSouth, which may be withheld.

D. **Binding Effect.** This Agreement will take effect when it has been signed by the authorized officers or representatives of both BancorpSouth and Customer.

Choice Escrow and Land Title, LLC *Customer*	**BancorpSouth Bank**
By: _______________ *Customer's Authorized Signature*	By: Ashley Kester *Bank's Authorized Signature*
Name: **L. Paige Payne** *Please Print*	Name: **Ashley Kester** *Please Print*
Title: **Branch Manager**	Title: **AVP**
Date: _______________	Date: _______________

FOR BANK USE ONLY

Company Tax Identification Number: 26-1724875

Lead DDA Account Number: _______________

Additional DDA Account Numbers: _______________

RECEIVED APR 23 2009

COPY

BANCORPSOUTH BANK
BUSINESS SERVICES AGREEMENT

THIS AGREEMENT made this 16th day of April, 2009, by and between BancorpSouth Bank, at and through its offices located at 3211 E Battlefield Springfield, MO 65804 (hereinafter "BancorpSouth"), and Choice Escrow and Land Title, LLC

☐ sole proprietorship ☐ partnership ☐ corporation ☒ other: LLC
with principal offices at 1440 E. Primrose Springfield, MO 65804
(hereinafter the "Customer").

BancorpSouth shall perform services described in separate Implementation Form(s) (hereinafter collectively the "Services"), in accordance with the terms and conditions of this Agreement and the respective Implementation Form(s). If the terms of the Form(s) conflict with the terms of this Agreement, the terms of the Form(s) shall apply.

1. **RELATED AGREEMENTS.** This Agreement shall be supplementary to, and be construed in conjunction with any and all other Account Agreement(s), ("Signature Cards"), Resolutions, Implementation Forms, Addendums, and other documents and agreements covering Customer's Account(s) with BancorpSouth. All such written agreements constitute the full and entire agreement regarding the Services. If the terms of this Agreement conflict with the terms of any other Account Agreement or Resolution associated therewith, the terms of such separate Account Agreement or Resolution shall control.

2. **SERVICES.** BancorpSouth shall perform Services in accordance with the terms and conditions of this Agreement and as more particularly described in separate Implementation Form(s). Implementation Form(s) shall constitute Customer's election as to specific Services offered hereunder and shall become effective as both parties hereto may execute one or more of same from time to time either contemporaneous herewith or hereafter; all of which shall constitute counterparts and exhibits to this Agreement. The Customer agrees that the Services to be performed by BancorpSouth will be used by the Customer solely for business or commercial purposes and not personal or consumer purposes.

3. **FEES.** The Customer shall pay for Services such fees in accordance with BancorpSouth's schedule of fees in effect from time to time (the "Fees"). A current schedule of Fees is available from BancorpSouth. Fees are also payable through the maintenance by Customer of compensating collected balances in specified account(s). The compensating collected balance requirement will be measured by BancorpSouth by profitability analysis of the Customer's specified account(s). Fees are payable monthly and BancorpSouth is authorized to charge the Fees on the due dates to specified

Revised 12/01/2006

000002817248754V901CMBSA
761724875

Exhibit 7

Customer account(s) or bill by monthly invoice, at its option. Fees, which are charged to a Customer's account, shall be reflected on Customer's monthly statement of account.

4. **CUSTOMER'S RECORDS AND MEDIA.** The Customer will provide BancorpSouth all records and data processing media necessary to perform the Services. The records will be legible, correct, complete and in the format specified on the Implementation Form(s). The records will contain all necessary information as determined by, and satisfactory to, BancorpSouth. All data processing media supplied by the Customer must be compatible with BancorpSouth systems and equipment. Checks will be MICR encoded according to BancorpSouth specifications.

If this Agreement is terminated, the Customer will notify BancorpSouth in writing within 30 days of the effective date of termination whether BancorpSouth should return or destroy any data processing media furnished by the Customer and any records in its possession or produced as a result of the expiring Services. If the Customer does not notify BancorpSouth within 30 days, BancorpSouth may destroy, retain or return any such material, as Customer would have then been deemed to have abandoned such media; therefore all risk of loss is with Customer and BancorpSouth shall have no responsibility for said media, or liability to Customer for same, if the media is destroyed, not returned, or otherwise dealt with by BancorpSouth.

All specifications, tapes or other media, and all programs and procedures utilized or developed by BancorpSouth in connection with the performance of the Services, are, will be and shall remain the sole property of BancorpSouth. In the event of termination of this Agreement, the Customer is responsible for their prompt return and shall return same, with any damages incurred in shipping and usage other than normal wear and tear being the sole responsibility of Customer.

5. **CUSTOMER'S FAILURE TO FURNISH SATISFACTORY RECORDS OR MEDIA.** BancorpSouth's performance is based on BancorpSouth receiving timely, accurate and complete data for each Service, acceptable to BancorpSouth, and which can be used on BancorpSouth systems or equipment. If any of these requirements are not met by the Customer, BancorpSouth shall:

a. no longer be bound to the normal delivery schedule;
b. be empowered to charge appropriate fees for the cost of converting nonstandard data into standard form, or complete missing data, in its discretion;
and/or
c. be authorized to deliver as complete and finished whatever portion of the Services can be performed with the data available.

6. **CUSTOMER'S DUTY TO INSPECT.** The Customer is responsible to inspect all Services performed when received and to notify BancorpSouth immediately of any errors. For daily Services, the Customer must give notice to BancorpSouth within a reasonable time after receipt of the material containing an error. The parties hereby mutually agree that a reasonable time to give notice to BancorpSouth shall be thirty (30)

days after receipt. Receipt shall mean actual delivery, if proof thereof is available to BancorpSouth; otherwise, receipt shall be deemed to have occurred three (3) banking days after the date of the material containing an error. A failure to give notice to BancorpSouth of error(s) within this time will relieve BancorpSouth of any and all liability.

7. **FACSIMILE SIGNATURE.** If the Customer at any time and in any manner, (including authorizations made by Account Agreement or Resolution), authorizes utilization of a facsimile signature, BancorpSouth shall be entitled to honor such facsimile signature for all purposes hereunder, including, but not limited to, charging Customer for such checks or other orders for payment of money so signed, regardless of by whom or what means the purported or actual facsimile signature may have been made or affixed thereto. Customer agrees and warrants that all previous and present authorizations are continued in full force and effect.

8. **LIMITATION OF LIABILITY.** It is understood that BancorpSouth will make reasonable best efforts to select and use facilities, equipment and personnel in connection with the Services to be performed under this Agreement so as to render error-free services. Otherwise, no warranties, express or implied, of any kind are offered or intended. BancorpSouth's sole responsibility for any error is to correct that error, provided BancorpSouth has received notice within a reasonable time, as specified in Section 6 hereof, for each Service. Correction of errors shall be Customer's sole and exclusive remedy. **BANCORPSOUTH HEREBY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, ARISING BY OPERATION OF LAW OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY AS TO MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.** Notwithstanding the foregoing, in the event BancorpSouth cannot correct an error, and solely in the event the Customer incurs a direct actual loss as a result thereof which is due to the negligence of BancorpSouth with respect to any entry or entries, BancorpSouth's maximum liability to the Customer shall be limited to (a) actual money damages not to exceed the actual money damages sustained and proven by the Customer, reduced on a comparative basis by the negligence, if any, of Customer, or (b) the total amount due from the Customer for the specific Services in connection with the uncorrected error(s) for the month during which those Services in connection with the uncorrected error(s) were performed, WHICHEVER IS LESS. In no event will BancorpSouth be liable or answerable to the Customer or any other party for any lost profits or any consequential, compensatory, punitive, special, or other damages caused by any error, act, delay or omission on BancorpSouth's part.

9. **INDEMNITY.** As long as BancorpSouth has performed as provided in Section 8 above, the Customer shall indemnify and hold BancorpSouth harmless from any and all claims, damages, losses, liabilities and cost or expenses, including reasonable attorneys' fees, which relate in any manner to the Services performed under this Agreement.

10. **TERMINATION.** This Agreement shall continue unless terminated (a) by either party upon thirty (30) days prior written notice to the other party, in which event

termination shall be deemed effective at the next statement cycle nearest to the expiration of the thirty (30) days notice of termination, as determined by BancorpSouth; (b) by BancorpSouth, if BancorpSouth determines in good faith that material just cause exists for terminating this Agreement (and in such event, BancorpSouth may terminate this Agreement at any time without notice to Customer); or (c) upon closing of any Account associated with the Services contemplated hereunder (and in such event, termination shall be immediate upon date of closure of such account).

11. **NOTICES.** Any notices and other communications required or permitted hereunder shall be in writing and shall be sent:

A. **To BancorpSouth at:**

ATTN: Treasury Management
(Department)

BancorpSouth Bank

3211 E. Battlefield
(Address)

Springfield, MO 65804
(City/State/Zip)

B. **To Customer at:**

ATTN: L. Paige Payne
(Name / Department)

Choice Escrow and Land Title, LLC
(Company)

1440 E. Primrose
(Address)

Springfield, MO 65804
(City/State/Zip)

Except as otherwise provided herein, notice shall be effective upon receipt.

12. **NON-PERFORMANCE/FORCE MAJEURE.** BancorpSouth shall bear no responsibility for non-performance of one or more Services caused by major events beyond its control, such as: fire, casualty, breakdown in equipment, lockout, strike, unavoidable accident, act of God, riot, war or the enactment, issuance or operation of any adverse governmental law, ruling regulation, order or decree, or emergency that prevents us from operating normally.

13. **MISCELLANEOUS.**

A. **Amendments.** This Agreement may not be amended except by mutual written agreement of the parties hereto.

B. **Governing Law.** This Agreement shall be governed by the laws of the State of location of the BancorpSouth branch identified in the Notice provision hereof, without regard to such state's conflicts of laws rules.

C. **Limitation and Assignment.** The parties acknowledge and agree that this agreement constitutes a contract to extend financial accommodations solely to and for the benefit of Customer. No third party beneficiary rights exist hereunder, nor are same intended. Customer rights and duties hereunder may not be assigned without the prior written consent of BancorpSouth, which may be withheld.

D. **Binding Effect.** This Agreement will take effect when it has been signed by the authorized officers or representatives of both BancorpSouth and Customer.

Choice Escrow and Land Title, LLC	BancorpSouth Bank
Customer	
By: [signature] *Customer's Authorized Signature*	By: [signature] *Bank's Authorized Signature*
Name: L. Paige Payne *Please Print*	Name: Ashley Kester *Please Print*
Title: Branch Manager	Title: AVP
Date:	Date:

FOR BANK USE ONLY

Company Tax Identification Number: 26-1724875

Lead DDA Account Number:

Additional DDA Account Numbers:

Exhibit 8

COPY

RECEIVED APR 23 2009

4406
KS

BANCORPSOUTH

INVIEW AUTOMATED INFORMATION REPORTING SERVICE IMPLEMENTATION FORM / ADDENDUM TO BUSINESS SERVICES AGREEMENT

This Addendum is between BancorpSouth Bank (referred to hereinafter as "BancorpSouth"), and Choice Escrow and Land Title, LLC

(referred to hereinafter as "Customer"). By signing below, both parties agree to be bound by the terms of this Addendum. This Addendum does not supersede any signature card rules, regulation or other agreements that Customer may have with BancorpSouth with respect to any accounts listed on InView Exhibit A - Account Information.

Description of Services - InView, BancorpSouth's Information Reporting System, provides both summary and detail information on Customer account activity. By utilizing Internet access on a personal computer, Customer may access the system to receive this information. Use of passwords provides protection and ensures confidentiality of Customer's data.

Security Procedures

1.1 Password and Risk of Loss – The Customer's authorized representatives as designated on InView Exhibit C - Company Profile and identified as Users on InView Exhibit A - Account Information shall be given a User ID(s) and Password(s) by BancorpSouth which will permit only these designated representatives to have access to InView. This User ID(s) / Password(s) shall not be disclosed by Customer and/or Customer's designated authorized representative to any other person(s). The User ID(s) / Password(s) will allow access to all functions provided by InView and selected by Customer including funds transfers. The User ID(s) / Password(s) may be coded by BancorpSouth to permit or restrict Customer's access or specific User's access per Exhibits A, B and/or C to this Addendum to any or all InView features, such as electronic funds transfers, wire transfers, account transfers, stop payment orders, positive pay services and account information. Customer assumes full responsibility and risk of loss resulting from, and BancorpSouth shall not be responsible and shall incur no liability to Customer for any risk of loss resulting from access gained, information disclosed or from transactions made on its account(s) through InView or otherwise by any person(s), whether or not such person(s) was authorized by Customer to make such transaction(s). It is Customer's responsibility to take all necessary precautions to safeguard the User ID(s) / Password(s), access codes and other security procedures and permit disclosure only to their authorized representatives. Customer will take all steps or actions necessary or advisable to protect the security of the InView System and the access code(s). Customer agrees to change its User Password(s) on a regularly scheduled basis, and BancorpSouth shall not be liable to Customer or any third party for any loss or damage resulting from or arising out of Customer's failure to do so. Customer shall immediately notify BancorpSouth if it knows or believes that InView or any access code is, has, or will be subject to unauthorized use. Customer will be liable to BancorpSouth for any loss, cost, expense or damage resulting from Customer's failure to do so and/or negligence in doing so.

1.2 Account Paths – Customer shall designate on InView Exhibit A - Account Information the Customer account(s) maintained with BancorpSouth to and from which funds transfers may be made. Any deposit account(s) accessible via InView may be designated by Customer to

Revised 1/24/2008

(0000026172487S4R001CMINVIEW

EXHIBIT "A"

permit no transfers or to permit transfers via InView as follows: (i) to the account; (ii) from the account; (iii) to and from the account; (iv) electronic transfers of funds into or out of Customer's accounts (s) at BancorpSouth or at any other financial institution as designated in Exhibit B – Multi-Bank Account Access; or (v) use InView for other services that BancorpSouth may develop and make available in the future. If the Wire Transfer Module is selected, Customer shall also designate all intended beneficiaries of any wire transfers and the beneficiaries' bank(s). Any attempt to transfer funds to or from account(s) or person(s) other than those designated may be rejected by BancorpSouth in its sole discretion.

While customer may use the InView System seven (7) days a week and twenty-four (24) hours a day, Customer acknowledges that some of InView's functions are not available at all times of the day or every day. To receive same banking day credit, Customer must make internal transfers (which are transfers between accounts located at BancorpSouth) on regular accounts between the hours of 12:01 AM and 7:00 PM Central Time (or the InView Regular Account Transfer Processing Deadline as may be amended from time to time, whichever is later) Monday through Friday (excluding bank holidays). The preceding statement does not apply to transfers made from accounts with secondary sources of funding; to receive same banking day credit for such transfers, Customer must make internal transfers (which are transfers between accounts located at BancorpSouth) between the hours of 12:01 AM and 4:00 PM Central Time (or the InView Zero-Balance Account Transfer Processing Deadline as may be amended from time to time, whichever is later) Monday through Friday (excluding bank holidays). Internal account transfers made after the applicable InView Regular Account Transfer Processing Deadline or Zero-Balance Account Transfer Processing Deadline, as both may be amended from time to time, will receive next banking day credit. To ensure the greatest likelihood of same banking day credit for internal account transfers, Customer should submit such transfers between the hours of 7:00 A.M. and the applicable InView Account Transfer Processing Deadline, as may be amended from time to time, Monday through Friday (excluding bank holidays). Notwithstanding the preceding guidelines, internal account transfers may be initiated by Customer between such times and during such non-business days, but BancorpSouth may be unable to give same day credit. Notwithstanding the foregoing, Customer acknowledges and agrees that any internal account transfers or electronic transfers shall not be effective until posted by BancorpSouth, after a reasonable time to post same, and all transactions, regardless of type, that are made after the applicable InView Account Transfer Processing Deadline, as may be amended from time to time, or on any non-business day will be processed as next banking day activity. The foregoing rules apply only to internal transfers involving accounts located at BancorpSouth. Outside account transfers involving accounts located at other financial institutions are subject to different processing and settlement deadlines, depending upon the type of transfer requested.

1.3 Changing Account Paths – Any request to change the designation of account(s) to or from which funds may be transferred must be submitted to BancorpSouth in writing and signed by a person authorized by Customer to make changes. BancorpSouth shall verify the requesting signature with the signature on file, and when corresponding signatures match, then, and only then, will any requested changes will be made.

1.4 On-Line Access – BancorpSouth shall provide to Customer on-line access to Customer's deposit and loan account(s) for the limited purposes of allowing Customer to access a balance and activity file for each deposit and loan account(s) held by Customer with

BancorpSouth. Such access shall be limited to providing Customer with daily balances on such deposit and loan account(s), checks presented or cleared, deposits made, fees assessed and such other transactions posted to Customer's deposit and loan account(s) as can be retrieved via InView as determined in the sole discretion of BancorpSouth.

1.5 Activity and Responsibility - Customer hereby authorizes BancorpSouth to honor, execute, and charge to Customer's account(s) any and all requests or orders to transfer or to pay funds through InView. The amounts of such transfers or payments shall be without limit, subject to available and collected funds. BancorpSouth is authorized to complete all such transactions on Customer's account(s), which are initiated through the use of Customer's access code.

Customer assumes full responsibility and risk of loss for all transactions made by BancorpSouth in good faith reliance upon Customer's requests or orders made through InView in accordance with the authorizations granted hereby and the procedures detailed herein, and the procedures set forth in the InView User Manual(s) and Help screens, as the same may be amended from time to time. Customer agrees that BancorpSouth shall be conclusively deemed to have discharged its duties to act in good faith and to exercise ordinary care if it has followed these procedures.

1.6 Loan Transactions – As part of the InView Service, Customer is hereby granted the use of the InView System for purposes of debiting/crediting the deposit account(s) listed in InView Exhibit A - Account Information in order to transfer funds from/to such deposit account(s) to/from any qualified loan account(s) of the Customer with BancorpSouth which the Customer listed in Exhibit A, but only for the purpose of advances/paydowns of principal only or regular, scheduled loan payments of principal and interest. Customer is granted the use of the InView System for the purpose of requesting an advance/paydown on any otherwise available and approved replenishing Line of Credit then in existence and in force with BancorpSouth. Advances may not be requested from non-replenishing lines of credit or regular term or installment loans; such loans may only receive payments via InView.

1.7 Wire Transfer Requests – Customer authorizes and requests BancorpSouth to make transfers of funds from time to time in accordance with the provisions and procedures set forth in BancorpSouth's Funds Transfer Agreement. Such transfers shall include transfers of Customer's funds from Customer's account(s) at BancorpSouth to Customer's account(s) at other depository institutions, and to account(s) of third parties at other depository institutions (See Repetitive Wire Transfer Set-Up Information). Requests from Customer to BancorpSouth shall be made by Customer's authorized representative(s) listed on the Funds Transfer Authorization furnished by Customer to BancorpSouth. To receive same banking day credit, Customer must submit wire transfer requests between the hours of 12:01 AM and 3:00 PM Central Time (or the InView Wire Transfer Processing Deadline as may be amended from time to time, whichever is later) Monday through Friday (excluding bank holidays). Wire transfer requests submitted after 3:00 PM Central Time (or the InView Wire Transfer Processing Deadline, as may be amended from time to time, whichever is later) will receive next banking day credit. To ensure the greatest likelihood of same banking day credit for wire transfer requests, Customer should submit wire transfer requests between the hours of 12:01 A.M. and 3:00 PM Central Time (or the InView Wire Transfer Processing Deadline, as may be amended from time to time, whichever is later), Monday through Friday (excluding bank holidays). Notwithstanding the preceding guidelines, wire

transfer requests may be initiated by Customer between such times and during such non-business days, but BancorpSouth may be unable to give same day credit. Notwithstanding the foregoing, Customer acknowledges and agrees that any wire transfer requests shall not be effective until posted by BancorpSouth, after a reasonable time to post same, and all such transactions that are made after 3:00 P.M. Central Time (or the InView Wire Transfer Processing Deadline, as may be amended from time to time, whichever is later) or on any non-business day will be processed as next banking day activity. Wire transfer requests subject to these terms include domestic wire transfers and international wire transfers paid in U.S. dollars. International wire transfers requiring conversion to foreign currency may not be placed through InView.

In addition to the Related Agreements per Customer's Business Services Agreement with BancorpSouth, this Addendum is subject to the Terms and Conditions in the Funds Transfer Agreement, and Funds Transfer Authorization executed by the Customer. Terms that are defined in the Funds Transfer Agreement and the Funds Transfer Authorization shall have the same meaning when used herein.

1.8 Stop Payment Orders - Subject to applicable law, Customer is deemed to have satisfied any legal requirement to confirm stop payment requests in writing if stop payments requests are entered by Customer via InView for checks or other items drawn on Customer's accounts with BancorpSouth. Customer is responsible for entering all stop payment data and verifying its accuracy. To be processed on the same banking day, Customer must submit stop payment requests between the hours of 12:01 AM and 7:00 PM Central Time (or the InView Stop Payment Processing Deadline as may be amended from time to time, whichever is later) Monday through Friday (excluding bank holidays). Stop payment requests submitted after 7:00 PM Central Time (or the InView Stop Payment Processing Deadline, as may be amended from time to time, whichever is later) will be posted on the next banking day. Notwithstanding the preceding guidelines, stop payment requests may be submitted by Customer between such times and during such non-business days, but BancorpSouth may be unable to process such requests on the same day. Notwithstanding the foregoing, Customer acknowledges and agrees that any stop payment requests shall not be effective until posted by BancorpSouth, after a reasonable time to post same, and all such transactions that are made after 7:00 P.M. Central Time (or the InView Stop Payment Processing Deadline, as may be amended from time to time, whichever is later) or on any non-business day will be processed as next banking day activity. All stop payment requests will expire not more than six (6) months from the date entered. Customer may renew stop payment requests for additional periods of six (6) months each by entering another stop payment request prior to the expiration of the current stop payment request.

1.9 Nondisclosure – Customer shall not sell, transfer, publish, disclose, divulge, furnish, display or otherwise make available any portion of InView, or InView documentation to others.

1.10 Company Administration Module / SuperUser Designation - Subject to any limitations on operating scope indicated on Exhibits A, B or C to the Addendum, persons who are designated on Exhibit C as SuperUsers shall have the authority to, from time to time, (a) add one or more Authorized Users to Exhibit C to the Addendum; (b) remove any one or more Authorized Users from Exhibit C to the Addendum; and (c) change for any one or more Authorized Users the scope of the Module Access designated for such Authorized User on Exhibit C to the Addendum (whether by broadening or restricting the scope thereof). As

used in the foregoing sentence, the term Authorized User shall not include any SuperUser. No SuperUser designated on Exhibit C to the Addendum may be removed as a SuperUser except by the execution by Customer and BancorpSouth of a new Exhibit C or SuperUser Amendment which supersedes and replaces this Addendum and/or any of its previously submitted Exhibits.

1.11 General - This Addendum is subject to the Terms and Conditions in the Business Services Agreement executed by the Customer. Terms that are defined in the Business Services Agreement shall have the same meaning when used herein.

This Addendum may be terminated by either party with thirty (30) days prior written notice to the other party. This Addendum may be amended only by written instrument executed by BancorpSouth and any authorized Customer representative on behalf of Customer.

All terms and conditions of this Agreement are agreed to as set forth this 16th day of April, 2009.

Choice Escrow and Land Title, LLC	BancorpSouth Bank
Customer	
By: [signature] Customer's Authorized Signature	By: [signature] Bank's Authorized Signature
Name: L. Paige Payne (Please Print)	Name: Ashley Kester (Please Print)
Title: Branch Manager	Title: AVP
Date:	Date:

Revised 1/24/2008

Exhibit 9

BANCORPSOUTH BANK
PO BOX 4023
SPRINGFIELD, MO 65808-4023
BRANCH 866

ACCOUNT NUMBER 618003800

ACCOUNT OWNER(S) NAME & ADDRESS

CHOICE ESCROW & LAND TITLE, LLC
TRUST ACCOUNT
ESCROW DISBURSEMENT ACCOUNT
1440 E. PRIMROSE
SPRINGFIELD, MO 65804

OWNERSHIP OF ACCOUNT - CONSUMER PURPOSE

☐ SINGLE-PARTY
☐ MULTIPLE-PARTY
☐ FIDUCIARY

☐ PAY-ON-DEATH DESIGNATION AS DEFINED IN THIS AGREEMENT
Name and Address of Beneficiaries:

TYPE OF ACCOUNT

☒ NEW ☐ EXISTING
☒ CHECKING ☐ SAVINGS
☐ MONEY MARKET ☐ ______
☐ NOW

ChexSystems ☐ Yes ☒ No
SSN Issued ______ State ______
NOT REQUIRED

OWNERSHIP OF ACCOUNT - COMMERCIAL PURPOSE

☐ SINGLE-PARTY ACCOUNT (Sole Proprietorship)
☐ CORPORATION
☐ PARTNERSHIP
☐ LIMITED PARTNERSHIP
☒ LIMITED LIABILITY COMPANY
☐ UNINCORPORATED ASSOCIATION
☐ FIDUCIARY
☐ GOVERNMENT
☐ OTHER ORGANIZATION

SIGNATURE(S) - The undersigned agree that this account is subject to and shall be governed by the deposit agreement entitled "Your Deposit Account Terms and Conditions" in effect at the opening of this account and as thereafter amended, replaced or superceded from time to time. The undersigned further authorize BancorpSouth Bank to verify credit and employment history and/or have a credit reporting agency prepare a credit report on the undersigned, as individuals. The undersigned acknowledge receipt of a copy of Your Deposit Account Terms and Conditions and the following disclosure(s), to all of which the undersigned agree to be bound:

☒ Account Information Statement ☒ Funds Availability
☐ Electronic Funds Transfer ☐ Truth in Savings ☐ Privacy
☐ ______
☐ ______

DATE OPENED 4/16/2009 BY CHANDA BURKE
INITIAL DEPOSIT $ $100.00
☐ CASH ☒ CHECK ☐ ______
HOME TELEPHONE # ______
BUSINESS PHONE # ______
DRIVER'S LICENSE # ______
E-MAIL ______
EMPLOYER ______
MOTHER'S MAIDEN NAME ______
Name and address of someone who will always know your location: ______

JIM A PAYNE
X ______

L PAIGE PAYNE
X ______

BROOKE L BLACK
X ______

CHRYSTAL D BOWLES
X ______

CARA THULIN
X ______

BACKUP WITHHOLDING CERTIFICATIONS

TIN: 26-1724875

☒ TAXPAYER I.D. NUMBER - The Taxpayer Identification Number shown above (TIN) is my correct taxpayer identification number.

☒ BACKUP WITHHOLDING - I am not subject to backup withholding either because I have not been notified that I am subject to backup withholding as a result of a failure to report all interest or dividends, or the Internal Revenue Service has notified me that I am no longer subject to backup withholding.

☐ EXEMPT RECIPIENTS - I am an exempt recipient under the Internal Revenue Service Regulations.

SIGNATURE: I certify under penalties of perjury the statements checked in this section and that I am a U.S. person (including a U.S. resident alien).

X ______ (Date) 4/16/2009

CUSTOMER COPY

Branch 866 Region 800
sgcd 1 0000061800380OIM4H901SIGCARD

AGREEMENT - These terms and conditions (this "Agreement") govern your deposit relationships with us unless varied or supplemented in writing by amendment as provided herein. Unless it would be inconsistent to do so, words and phrases used in this document should be construed so that the singular includes the plural and the plural includes the singular. As used in this Agreement, the "account" means each deposit account you maintain with us other than Time Deposit (Certificate of Deposit) accounts and Individual Retirement Accounts; "we," "our," or "us" mean BancorpSouth Bank; "you" or "your" mean the owner(s) of the account; and "signature page" means the page(s) containing the signatures of the owner(s) of the account. This Agreement applies separately to each account. The account may not be transferred, pledged or assigned without our written consent, and we reserve the right to withhold such consent for any reason.

Much of our relationship with our deposit customers is regulated by state and federal law, especially the law relating to negotiable instruments, the law regulating the methods of transferring property upon death and the rights of surviving spouses and dependents, the law pertaining to estate and other succession taxes, the law regarding electronic funds transfer, and the law regarding the availability of deposited funds. This body of law is too large and complex to be reproduced here.

The purpose of this Agreement is to:

(1) summarize the rules applicable to the more common transactions;

(2) establish rules to govern transactions or circumstances which the law does not regulate; and

(3) establish rules for certain events or transactions which the law already regulates but permits variation by agreement.

LIABILITY - Each of you agrees, for yourself (and the person or entity you represent if you sign as a representative of another) to the terms and conditions set forth in this Agreement and the schedule of charges that may be imposed. You authorize us to deduct these charges as accrued directly from the account balance. You also agree to pay additional reasonable charges we may impose for services you request which are not contemplated by this Agreement. Each of you also agrees to be jointly and severally (solidarily) liable for any account deficit resulting from charges or overdrafts, whether caused by you or another authorized to withdraw from the account, and the costs we incur to collect the deficit including our reasonable attorneys' fees.

DEPOSITS - Any items, other than cash, accepted for deposit (including items drawn "on us") will be given provisional credit only until collection is final (and actual credit for deposits of, or payable in, foreign currency will be at the exchange rate in effect on final collection in U.S. dollars). Applicable law may require us to make your deposits available for withdrawal before payment becomes final or before the expiration of other banks' deadlines to return your deposited items to us for refund. You agree that our making all or any part of a deposit available to you for withdrawal is not a waiver of our right to charge back to the account any deposited item which is returned to us unpaid or for refund; instead, we may charge back to the account, and you will be responsible for, all such items. Subject to any other limitations, interest will be paid only on collected funds, unless otherwise provided by law. All transactions received after our daily cut-off time on a business day we are open (a "banking day"), or received on a day in which we are not open for business, will be treated and recorded as if initiated on the next following banking day. Our daily cut-off time varies from location to location and is posted at each of our locations.

WITHDRAWALS - Any one of you who signs the signature page, including authorized signers, may withdraw or transfer all or any part of the account balance at any time on forms approved by us. However, we reserve the right to limit the amount of any withdrawal in cash where, for example, currency in the amount of the withdrawal is not available at our branch or your withdrawal exceeds the amount we allow via automatic teller machine or if the cash supply of the automatic teller machine is depleted. Each of you authorizes each other person signing the signature page to endorse any item payable to you or your order for deposit to the account or any other transaction with us. You agree that our right to charge a check against the account does not depend on the date of the check. Therefore, we may charge a check against the account before the date of the check or at any time thereafter, provided, however, that we may, but are not required to, refuse to pay a check which appears on its face to be more than six months old. In any event, we will not be liable to you for charging against the account a check before its date or after it is more than six months old. The fact that we may honor withdrawal requests which overdraw the finally collected account balance does not obligate us to do so. Withdrawals will first be made from collected funds, and we may, unless prohibited by law, refuse any withdrawal request against uncollected funds, even if our general practice is to the contrary. We reserve the right to refuse any withdrawal or transfer request which is attempted by any method not specifically permitted, which is for an amount less than any minimum withdrawal requirement, or which exceeds any frequency limitation. Even if we honor a nonconforming request, we may close the account in the event of repeated abuse of the stated limitations. We will use the date a transaction is completed by us (as opposed to the day you initiate it) to apply the frequency limitations. On interest bearing accounts other than time deposits, we reserve the right to require at least seven days' written notice before any withdrawal or transfer.

ACH, WIRE AND FUNDS TRANSFERS - We may decline to process any wire or funds transfer which is not subject to Regulation E or the Electronic Funds Transfer Act until you enter into a separate Funds Transfer Agreement with us. If we process any wire or funds transfer for you before you enter into a separate Funds Transfer Agreement, with respect to each such transfer you will be bound by the terms of this section. You agree to be bound by all rules and regulations governing any system through which any transfer occurs, including, but not limited to, any ACH rules, NACHA rules and the rules and regulations pertaining to Fedwire, the electronic transfer system of the Federal Reserve Banks. We may make wire or funds transfers by any means available to us, including, but not limited to, through our correspondent banks or by internal book entry. We have no obligation to notify you of incoming wire or funds transfers. Any credit for incoming wire or funds transfers is provisional until we have received final payment. If we do not receive final payment, we may reverse the credit. We may permit any of you or any authorized signer to order wire or other funds transfers from the account by telephone, in person, by written instruction, or by any other means acceptable to us, subject to any time deadlines or other conditions or procedures which we may establish. Wire and funds transfers are made only through the use of identifying numbers for the recipient bank and account, without regard to any names which may be furnished for any recipient bank or account. You must furnish the correct identifying numbers to us in connection with each wire or funds transfer. Funds will be wired or transferred in accordance with the identifying numbers you furnish us (or the identifying numbers which you use, if you are originating an ACH transaction), even if an identifying number is incorrect or is inconsistent with any name you may use or furnish us. In such event, we will not be responsible for your error, the transfer will not be considered an unauthorized transaction, and any loss will be entirely yours. Any instructions you may give us in connection with a wire or funds transfer will not be binding on us unless we have agreed to such instructions in writing. You must strictly observe all deadlines we impose for the processing of wire and funds transfers. We will not be responsible for any delay or other consequences which result from your failure to comply with any of these deadlines. You have no right to cancel or change any wire or funds transfer after you submit it to us. Any attempt by us to cancel or change or any wire or funds transfer at your request will not constitute the assumption of any duty by us. You assume all risk associated with international wire or funds transfers. We will not be liable to you in any way in connection with an international wire or funds transfer, whether for failure of delivery, delayed delivery, fluctuations in exchange rates or for any other reason. If any incoming wire or funds transfer is denominated in a foreign currency, you authorize us to convert such to U. S. Dollars according to such exchange rate which we may select at our discretion. You acknowledge and agree that such exchange rate may not be the most favorable rate of exchange published and that you will be bound by our choice of exchange rate. If you provide your account number or any other account identifying information to any third party and such third party originates any funds transfer transaction on the account, you agree that we may treat such transaction as a transaction authorized by you.

OWNERSHIP OF ACCOUNT AND BENEFICIARY DESIGNATION - You intend these rules to apply to the account depending on the form of ownership and beneficiary designation, if any, specified on the signature page. We make no representations as to the appropriateness or effect of the ownership and beneficiary designations, except as they determine to whom we pay the account funds. Single Party Account - Is owned by one person. Multiple Party

Account - is owned by two or more persons jointly with right of survivorship and not as tenants in common, regardless of the conjunction ("or", "and") used between the depositors' names. Each of you expressly agrees that the account is not owned as a tenancy by the entireties. Each of you intends that upon your death the balance in the account (subject to any previous pledge to which we have consented) will vest in and belong to the survivor(s) as the separate property and estate of such survivor(s). If two or more of you survive, you will own the balance in the account as joint tenants with survivorship and not as tenants in common. Transactions on Multiple Party Accounts do not require the signatures of all account owners to transact on the account. Instead, any one account owner or authorized signer may transact on the account to the exclusion of the other(s), and each of you authorize each other of you to do so without further consent. If this Agreement is governed by the laws of the state of Louisiana, the owners of a Multiple Party Account are co-owners of the account, and all or any part of any deposit may be paid to any one of you, whether any other of you is living or not, and any such payment to any of you shall constitute receipt and acquittance and shall fully release and discharge us from the claims of any person to funds of the deceased depositor for the payment made. Pay On Death Account - Pay-On-Death beneficiaries acquire the right to withdraw only if: (1) all persons creating the account die, (2) the beneficiary is then living, and (3) we are not otherwise required by law to make payment to some other person. If two or more beneficiaries are named and survive the death of all persons creating the account, such beneficiaries will own the account and may transact on it according to the Multiple Party Account rules stated above unless otherwise provided by law. Any one account owner or authorized signer may: (1) change beneficiaries, (2) change account types, and (3) withdraw all or part of the deposit at any time. If two or more of you create such a Pay-On-Death Account, you own the account according to the Multiple Party Account rules stated above until the last of you dies. Fiduciary Account - A Fiduciary Account, whether for a consumer or a commercial purpose, is one in which the person controlling the account does so for the benefit of another. Examples of fiduciaries are trustees, executors, conservators, custodians for minors, representative payees and court-appointed guardians. For purposes of this Agreement, guardians such as parents or other relatives who have not been court-appointed or persons who have not complied with necessary provisions of any applicable transfer to minors laws are not fiduciaries. We are not a fiduciary in connection with the account. For fiduciary accounts, we will usually require, in the case of trustees, a trust resolution according to our form, and in all other cases documents evidencing the fiduciary's authority. We have no duty to inspect any will or trust document, and you agree that we will not be bound by any limitations imposed in a will or trust document. You agree that a Fiduciary Account is a general deposit and not a special deposit. Corporation, Partnership, LLC, Government and other Organizational Accounts - We will usually require a separate resolution in a form acceptable to us designating the person(s) permitted to make withdrawals from any account in the name of a legal entity such as a partnership, corporation, LLC, governmental entity or other organization.

STOP-PAYMENTS - A stop-payment order must be given in the manner required by law and must be received in time to give us a reasonable opportunity to act on it before our stop-payment cut off time. Our stop-payment cut off time is one hour after the opening of the next banking day after the banking day on which we receive the item. Additional limitations on our obligation to stop-payment are provided by law. A stop-payment order must precisely identify the number, date and amount of the item, and the payee. We will honor a stop-payment request by the person who signed the particular item, and, by any other person, even though such other person did not sign the item, if such other person has an equal or greater right to withdraw from the account than the person who signed the item in question. A release of the stop-payment request may be made only by the person who initiated the stop-payment.

AMENDMENTS AND TERMINATION - We may change, in whole or in part, any term of this Agreement or any of the disclosures indicated on the signature page or previously given to you. Rules governing changes in interest rates have been provided separately. For other changes we will give you reasonable notice in writing or by any other method permitted by law. We may also close the account at any time upon reasonable notice to you and tender of the account balance personally or by mail. Notice from us to any one of you is notice to all of you unless otherwise provided by law.

STATEMENTS - You must examine your statement of account with reasonable promptness. If you discover (or reasonably should have discovered) any forgeries, unauthorized payments, alterations or disputed transactions, you must promptly notify us of the relevant facts. Even if you do promptly notify us, you still may have to either share the loss with us or bear the loss entirely yourself (depending on whether you exercised ordinary care or substantially contributed to the loss). The loss could be not only with respect to items on the statement but other items forged or altered by the same wrongdoer. You agree that the time you have to examine your statement and report to us will not, in any circumstance, exceed a total of 60 days from when the statement is first made available to you.

You further agree that if you fail to report any unauthorized signatures, alterations, forgeries, unauthorized activity or any other errors or disputed transactions in the account within 60 days of when we make the statement available, you cannot assert a claim against us on any items in that statement, and the loss will be entirely yours.

You also agree to examine your statement with the same reasonable promptness to discover whether any deposit is missing or has been incorrectly credited. If your statement of account contains any error pertaining to any deposit, and if you fail to report such error to us within 60 days of when we make the statement available, you cannot assert a claim against us for such error, and any loss will be entirely yours.

The 60 day limitations set forth in this section are without regard to whether we exercised ordinary care.

If the account is a commercial purpose account, you additionally agree to take advantage of products and services we offer for the detection and prevention of fraud and unauthorized transactions, such as "Positive Pay" cash management products. If you fail to utilize any such product or service, you agree that you will be precluded from asserting any claim against us for any unauthorized transaction which could have been prevented by the proper use of such product or service.

We may require any report of errors on your statement to be put in writing by you and we may additionally require you to furnish us with an affidavit concerning the error on forms acceptable to us. If the account is a commercial purpose account, you agree to exhaust all rights against any insurance coverage you may have before making any claim against us. Our liability to you, if any, will be reduced by the amount of any insurance you are entitled to receive. You agree, upon request by us, to assign to us all insurance rights you may have in connection with any loss on your commercial purpose account.

DIRECT DEPOSITS - If, in connection with a direct deposit plan, we deposit any amount in the account which should have been returned to the Federal Government for any reason, you authorize us to deduct the amount of our liability to the Federal Government from the account or from any other account you have with us, without prior notice and at any time, except as prohibited by law. We may also use any other legal remedy to recover the amount of our liability.

TEMPORARY ACCOUNTS - If you intend for the account to be a Multiple Party Account, but all of you are not present at the time the account is opened, we may permit as many of you as are present to open the account either as a Single Party Account or a Multiple Party Account only in the name(s) of those who are present (the "Temporary Account"). At the same time we may permit as many of you as are present to also sign account documentation listing the names of all those intended to be owners of the Multiple Party Account, including those who are not present (the "Permanent Account"). However, we are not required to give effect to the Permanent Account documentation until all owners listed on such documentation have signed it and we have processed it, at which point the Permanent Account documentation shall supersede and replace the Temporary Account documentation. Notwithstanding the foregoing sentence, we may give the Permanent Account documentation retroactive effect to the date on which the Temporary Account was opened. We are not required to give any of you notice that the Permanent Account documentation has taken effect, nor are we required to give any intended owner notice that such intended owner's signature is needed on the Permanent Account documentation. If the Permanent Account documentation is not signed by all intended owners within 30 days following the opening of the Temporary Account, we may discard the Permanent Account documentation and will have no liability for doing so. A Temporary Account is subject to all of the terms and provisions of this Agreement.

SET OFF - You each agree that we may without prior notice to you set off the funds in the account against any due and payable debt owed to us now or in the future, by any of you having the right of withdrawal, to the extent of such persons' or legal entity's right to withdraw. If the debt arises from a note, "any due and payable debt" includes the total amount of which we are entitled to demand payment under the terms of the note at the time we set off, including any balance the due date for which we properly accelerate under the note. This right of set-off applies regardless of the source of the deposit, and you consent that we may exercise this right of set-off against deposits which consist in whole or in part of government payments, including, but not limited to, Social Security and Veterans Administration payments. This right of set-off does not apply to the account if: (a) it is an Individual Retirement Account or other tax deferred retirement account, or (b) the debtor's right of withdrawal arises only in a representative capacity. We will not be liable for the dishonor of any check when the dishonor occurs because we set off a debt against the account. You agree to hold us harmless from any claim arising as a result of our exercise of our right of set-off.

FACSIMILE SIGNATURES - You authorize us, at any time, to charge you for all checks, drafts, or other orders or transactions, for the payment of money, that are drawn on us by facsimile signature, regardless of by whom or by what means the facsimile signature(s) may have been affixed.

AUTHORIZED SIGNERS - An authorized signer is someone you designate to conduct transactions on your behalf, but does not have any ownership or rights in the account unless the authorized signer is also named as a Pay on Death beneficiary, in which case the Pay-On-Death Account rules apply. Otherwise, the rights of an authorized signer cease upon your death but not upon your disability or incapacity; however, you agree that we will not be liable for honoring any transaction by an authorized signer after your death. We reserve the right to limit the number of authorized signers and to decline to permit authorized signers on certain types of accounts.

ACCOUNTS OWNED BY MINORS - If this is a Multiple Party Account and one or more of the account owners is a minor, all adult owners of the account jointly and severally agree that all transactions made on the account by any such minor shall be deemed to have been made by such adult owners, regardless of whether any such transaction may be void or voidable. EACH SUCH ADULT OWNER AGREES TO INDEMNIFY US AND HOLD US HARMLESS FROM ANY LOSS WE INCUR IN CONNECTION WITH ANY TRANSACTION MADE BY ANY SUCH MINOR.

REFUSAL OF DEPOSITS - We may refuse to accept any item, wire or electronic funds transfer for deposit or to send any item for collection, and we will have no liability to you or to any other person for such refusal.

ORDER OF PAYMENT - Unless otherwise provided in the Account Information Statement (see OTHER TERMS section below), if more than one item or order is presented for payment against the account on the same day and the available balance of the account is insufficient to pay them all, we may pay any of them in any order we choose, even if the order we choose results in greater insufficient funds fees than if we had chosen to pay them in some other order. Our payment of any item or order in overdraft does not create any obligation for us to pay any other item or order in overdraft in the future, and you agree that no course of dealing regarding the payment of items or orders in overdraft will be created between us.

ERRORS - If there occurs any error on the account in your favor, such as crediting the account for any amount to which you are not entitled, charging the account for an amount less than the amount of an item or other order, or receipt of any direct deposit to which you are not entitled, you agree that we may adjust this account to correct the error and that, if there are insufficient funds in the account for such adjustment, you will immediately pay us the amount necessary to correct the error. You agree to pay our reasonable attorneys' fees and expenses in the event we sue you to recover the amount necessary to correct the error.

DEPOSITS NOT MADE IN PERSON - We are not responsible for transactions initiated by mail, outside depository or left with us for subsequent processing until we actually record them, and you accept and assume all risks inherent in initiating such transactions. For deposits so initiated, our determination of the amount of the deposit will be conclusive, and you waive any right to contest our determination.

RESTRICTIVE LEGENDS - For your own purposes you may print or write on checks or other items restrictive legends specifying the number of signatures required, the maximum amount for which the check or item is payable, the number of days the check or item is valid and similar restrictions. However, you agree that such restrictions shall not be binding on us, that we may disregard such restrictions and that we will have no liability to you or to any other person for paying any check or other item inconsistently with any restrictive legend that is printed or written thereon.

CHECK CHARACTERISTICS - If you use checks from sources other than vendors approved by us, or if you use check stock, security features or ink color which cause data to disappear or to become obscured when the check is converted into an image, you agree to bear any loss which results. We will not be liable for failing to honor a stop-payment order for an item issued on a check form from sources other than vendors approved by us.

SECURITY INTEREST - In addition to the rights of set-off which we have under this Agreement, you hereby grant to us a security interest in the account to secure payment of any obligation which you now owe us or which you may owe us at any time in the future, including your obligation to pay our attorneys' fees and expenses and your obligation to indemnify us as provided elsewhere in this Agreement. When any such obligation is due and payable to us, we may pay such obligation, or any part thereof, from the account without prior notice to you, and we will not be liable for the dishonor of any item or order which results from such exercise of our security interest. If the account has any pay-on-death beneficiary, the interests of such beneficiary shall be junior to our security interest and shall be subject to our right of set-off, even if we do not exercise our security interest or right of set-off until after your death.

PAYMENT TO BENEFICIARIES - Payment to pay-on-death beneficiaries shall be as provided by law. Notwithstanding anything in the Pay-on-Death Account rules stated above, we may require any pay-on-death beneficiary wishing to continue transactions with us to close the account and open a new account under such beneficiary's signature.

INDEMNIFICATION BY FIDUCIARY - IF THE ACCOUNT IS A FIDUCIARY ACCOUNT (INCLUDING, BUT NOT LIMITED TO, AN ACCOUNT USED AS A CUSTODIAL ACCOUNT OR AS A REPRESENTATIVE PAYEE ACCOUNT TO RECEIVE PAYMENTS FROM THE SOCIAL SECURITY ADMINISTRATION OR ANY OTHER GOVERNMENTAL PAYOR), YOU, THE FIDUCIARY, AGREE IN YOUR INDIVIDUAL CAPACITY TO INDEMNIFY US AND HOLD US HARMLESS FROM ANY LOSS WE INCUR IN CONNECTION WITH THE ACCOUNT, WHETHER RESULTING FROM OVERDRAFT, ERROR IN YOUR FAVOR, RECLAMATION BY ANY GOVERNMENTAL PAYOR, ANY DISPUTE WITHIN THE SCOPE OF THE "ACCOUNT DISPUTE; INDEMNITY; LIMITATION ON LIABILITY" SECTION BELOW OR ANY OTHER REASON. IN THE EVENT OF ANY SUCH LOSS, WE MAY ENFORCE THE FOREGOING INDEMNITY BY SETTING OFF THE AMOUNT OF SUCH LOSS AGAINST (OR BY EXERCISING ANY SECURITY INTEREST WE MAY HAVE IN) ANY OTHER ACCOUNT WITH US IN WHICH YOU, THE FIDUCIARY, HAVE AN INTEREST (UNLESS YOUR INTEREST IN SUCH ACCOUNT IS ONLY AS A FIDUCIARY), AND WE WILL NOT BE LIABLE TO YOU OR TO ANYONE ELSE FOR THE DISHONOR OF ANY ITEM OR ORDER ON SUCH OTHER ACCOUNT WHICH RESULTS FROM SUCH SET-OFF OR EXERCISE OF OUR SECURITY INTEREST.

SIGNATURE BY MARK - If any signature which appears on the signature page is by mark (such as an "X"), then you agree that we will have no liability whatsoever on claims by you or any other person based on forgery, unauthorized signature, alteration or the like.

ACCOUNT DISPUTE; INDEMNITY; LIMITATION ON LIABILITY - IN THE EVENT OF ANY DISPUTE REGARDING THE ACCOUNT, INCLUDING ANY DISPUTE OVER OWNERSHIP OF OR ENTITLEMENT TO THE ACCOUNT OR THE CAPACITY OR AUTHORITY OF ANY PERSON TO TRANSACT ON THE ACCOUNT, YOU AGREE TO PAY OUR REASONABLE ATTORNEYS' FEES AND EXPENSES IN THE EVENT THAT WE BECOME INVOLVED IN ANY PROCEEDING TO RESOLVE SUCH DISPUTE. IN THE EVENT OF SUCH DISPUTE WE MAY PAY THE AVAILABLE BALANCE OF THE ACCOUNT INTO COURT, AND IN THAT EVENT YOU AGREE NOT TO MAKE ANY CLAIM AGAINST US. ADDITIONALLY, TO THE EXTENT PERMITTED BY LAW, YOU AGREE TO INDEMNIFY US, OUR DIRECTORS, OFFICERS, EMPLOYEES AND AGENTS FROM AND AGAINST ANY AND ALL CLAIMS ARISING FROM OR IN ANY WAY RELATING TO ANY SUCH DISPUTE. YOU ALSO AGREE THAT WE SHALL BE ENTITLED TO RECOVER OUR REASONABLE ATTORNEY'S FEES AND EXPENSES IN CONNECTION WITH SUCH PAYMENT INTO COURT AND THAT WE MAY RECOVER SUCH FEES AND EXPENSES FROM THE BALANCE PAID INTO COURT.

IN THE EVENT OF ANY KIND OF CLAIM BY YOU AGAINST US IN CONNECTION WITH THE ACCOUNT, YOU AGREE THAT WE WILL NOT BE LIABLE TO YOU FOR ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY OR PUNITIVE DAMAGES.

GOVERNING LAW; PROCESS; REPRESENTATIVES - With regard to any account established online, this Agreement is governed by the laws of Mississippi and by federal law and regulation. Otherwise, this Agreement is governed by the laws of the state of the location of our branch identified on the signature page and by federal law and regulation. Notwithstanding this, we may honor any levy, attachment, garnishment, execution, subpoena, court order, administrative order (including child support order) or other legal process which names you or which encompasses you, the account or any tax identification number associated with the account, regardless of whether we are subject to the jurisdiction of the issuer of such, regardless of in which state such is served on us and regardless of how such is served on us. We are not required to raise any defense in your behalf. We may also comply with the directions of any executor, administrator, conservator, guardian, receiver, bankruptcy trustee, attorney-in-fact or any other such representative purporting to have authority over the account who furnishes us with apparently authentic copies of documents which confer such authority. We may refuse to deal with any such representative in our sole discretion, and we will not be liable to you for such refusal. You agree that we may place temporary or permanent holds on the balance of the account related to or otherwise in response to any such process or authority and that we shall be fully protected in doing so, even if we later determine that such process or authority is inapplicable to the account. YOU AGREE THAT WE WILL NOT BE LIABLE TO YOU OR TO ANY OTHER PERSON FOR ACTING OR NOT ACTING ON ANY SUCH PROCESS OR FOR ACTING OR NOT ACTING ON THE DIRECTIONS OF ANY SUCH REPRESENTATIVE OR FOR PLACING OR NOT PLACING TEMPORARY OR PERMANENT HOLDS, AND YOU AGREE TO INDEMNIFY US, OUR DIRECTORS, OFFICERS, EMPLOYEES AND AGENTS FROM AND AGAINST ANY AND ALL CLAIMS ARISING FROM OR IN ANY WAY RELATING TO SUCH ACTION OR INACTION.

EFFECT OF TERMINATION OR AMENDMENT - Termination of the account, whether by us or by you, does not relieve you of any obligation you may then owe us. We may accept deposits to the account after it has been closed in order to collect any deficit balance, and such acceptance will not constitute reinstatement of the account. Your use of the account after we give you notice of any amendment to this Agreement constitutes your acceptance of such amendment. No amendment of this Agreement is enforceable against us unless it is in writing and we have authored the writing or have signed it through an employee having authority to do so, such as a regional president. No practice or course of dealing in connection with the account which is at variance with this Agreement shall constitute a modification or amendment of this Agreement.

OTHER TERMS - The account is additionally governed by our Account Information Statement. You acknowledge receipt of a copy of the Account Information Statement and you agree to be bound by its terms, as amended by us from time to time, and to be responsible for all fees and charges set forth therein which apply to the account. You understand that the Account Information Statement does not necessarily set forth all possible fees and charges which apply to the account.

SEVERABILITY - In the event that any part of this Agreement is determined to be unenforceable, such will not affect the other parts of this Agreement, all of which shall remain fully enforceable.

ARBITRATION - IF THE ACCOUNT IS A COMMERCIAL PURPOSE ACCOUNT, THEN YOU AGREE THAT ANY CLAIM, DISPUTE OR CONTROVERSY ("CLAIM") BY EITHER YOU OR US AGAINST THE OTHER, OR AGAINST THE EMPLOYEES, AGENTS OR ASSIGNS OF THE OTHER, ARISING FROM OR RELATING IN ANY WAY TO THIS AGREEMENT, THE ACCOUNT OR ANY TRANSACTION, INCLUDING CLAIMS REGARDING THE APPLICABILITY OF THIS ARBITRATION CLAUSE OR THE VALIDITY OF ALL OR ANY PART OF THIS AGREEMENT, SHALL BE RESOLVED BY BINDING ARBITRATION BY THE NATIONAL ARBITRATION FORUM, UNDER THE CODE OF PROCEDURE IN EFFECT AT THE TIME THE CLAIM IS MADE OR FILED. RULES AND FORMS OF THE NATIONAL ARBITRATION FORUM MAY BE OBTAINED AND CLAIMS MAY BE FILED AT ANY NATIONAL ARBITRATION FORUM OFFICE, WWW.ARBITRATION-FORUM.COM OR POST OFFICE BOX 50191, MINNEAPOLIS, MINNESOTA 55405, TELEPHONE 1-800-474-2371. ANY ARBITRATION HEARING AT WHICH YOU APPEAR WILL TAKE PLACE IN THE CITY WHICH IS THE LOCATION OF OUR BRANCH AT WHICH THE ACCOUNT WAS OPENED. THIS ARBITRATION AGREEMENT IS MADE PURSUANT TO A TRANSACTION INVOLVING INTERSTATE COMMERCE AND SHALL BE GOVERNED BY THE FEDERAL ARBITRATION ACT, 9 U.S.C. SECTIONS 1-16. JUDGMENT UPON ANY ARBITRATION AWARD MAY BE ENTERED IN ANY COURT HAVING JURISDICTION. IN THE ABSENCE OF THIS ARBITRATION AGREEMENT YOU AND WE MAY OTHERWISE HAVE HAD A RIGHT OR OPPORTUNITY TO LITIGATE CLAIMS THROUGH A COURT AND/OR TO PARTICIPATE OR BE REPRESENTED IN LITIGATION FILED IN COURT BY OTHERS, BUT EXCEPT AS OTHERWISE PROVIDED ABOVE, ALL CLAIMS MUST NOW BE RESOLVED THROUGH ARBITRATION.

Exhibit 10

MEMO

To: Treasruy Management
From: Choice Escrow and Land Title, LLC
Re: Waiver Consent – InView Wire Module Dual Control

We, Choice Escrow and Land Title, LLC, and all related entities we manage which utilize BancorpSouth's InView Wire Module to transact online wire requests, understand the additional risk we assume by waiving BancorpSouth's requirement to utilize Dual Control for Outgoing Wires. By signing below we understand that although InView can restrict the account from which wires are sent and the amount related to said wire, InView **CANNOT** restrict to where the wire is sent.

Since we wish to waive Dual Control anyone who has a User ID and Password or obtains access to a User ID and Password can wire funds to any other financial institution without restriction by BancropSouth or the InView system. We understand that this can also occur if our password is stolen. Further, if funds are fraudulently wired out in this manner there is a substantial possibility that we will be unable to retrieve our funds or recover losses.

The related account(s) accessible via BancorpSouth's InView Wire Module is/are:

XXXXXXXXXXX 618003800
XXXXXXXXXXX ______
XXXXXXXXXXX ______

(must be ten digits)

We agree this waiver applies only to the wires initiated through InView. If we initiate a wire through one of BancorpSouth's branches we will follow the customary guidelines and procedures required and use an assigned pin number, if previously provided.

Thank-you,

X

Authorized Signature

L. Paige Payne
Printed Name

Branch Manager
Title

05/06/09
Date

InView Wire Transfer User Security Form

Exhibit 11

Instructions:

- This form must be printed, completed in writing, and signed by an authorized company officer.
- Enter the company name at the top of the form. On each row below, list a user name, and indicate what wire transfer capabilities the user should be given by placing a checkmark in the appropriate column(s).
    - "Dual Control" means that a user cannot approve and release the same wire transfer; another user would have to release the wire transfers placed by a user who is subject to dual control. Note that if a user does not have both approve and release capability, dual control should not be checked, as it would serve no purpose.
    - If desired, list a daily wire transfer limit that should apply to the user; when this daily limit is reached, the user may not approve or release additional wire transfers on that day. (Note: Regardless of user limits for higher amounts, an account's current ledger balance will govern whether or not a wire transfer can be processed.)
- If a user should have the same wire transfer capabilities for all accounts, place a checkmark in the "All" column; otherwise, list the specific account number to which the capabilities apply. If a user needs different wire transfer capabilities on different accounts, list the user's name as many times as necessary to specify the different capabilities per account.

Choice Escrow and Land Title, LLC
Company Name

User ID Or User Name:	Wire Transfer Capabilities: None	Enter	Approve	Release	Cancel	Templates	Dual Control	User Daily Wire Transfer Limit (List One Amount Per Username)	Accounts: All	Specific:
Brooke Black	☐	☒	☒	☒	☒	☒	☐		☐	618003800
Cara Thulin	☐	☒	☒	☒	☒	☒	☐		☐	618003800
	☐	☐	☐	☐	☐	☐	☐		☐	
	☐	☐	☐	☐	☐	☐	☐		☐	
	☐	☐	☐	☐	☐	☐	☐		☐	
	☐	☐	☐	☐	☐	☐	☐		☐	
	☐	☐	☐	☐	☐	☐	☐		☐	
	☐	☐	☐	☐	☐	☐	☐		☐	
	☐	☐	☐	☐	☐	☐	☐		☐	
	☐	☐	☐	☐	☐	☐	☐		☐	
	☐	☐	☐	☐	☐	☐	☐		☐	
	☐	☐	☐	☐	☐	☐	☐		☐	
	☐	☐	☐	☐	☐	☐	☐		☐	
	☐	☐	☐	☐	☐	☐	☐		☐	
	☐	☐	☐	☐	☐	☐	☐		☐	
	☐	☐	☐	☐	☐	☐	☐		☐	
	☐	☐	☐	☐	☐	☐	☐		☐	
	☐	☐	☐	☐	☐	☐	☐		☐	
	☐	☐	☐	☐	☐	☐	☐		☐	

Company Daily Wire Transfer Limit: $ N/A

If desired, enter a daily wire transfer limit to apply at the company level. When this daily limit is reached, users at the company may not approve or release additional wire transfers on that day. (Note: Regardless of company or user limits for higher amounts, an account's current ledger balance will govern whether or not a wire transfer can be processed.)

X [signature]
Authorized Signature

05/06/09
Date

Statement

Balance Statement for Trust Account
Account Number 0618003800

Balance Statement Period: 03/17/2010 through 03/17/2010

Balance Date As Of	03/17/2010
Ledger Balance	$349,352.20
Collected Balance	$349,352.20
MTD Average Collected Balance	$1,059,205.97
One Day Float	$0.00
Two + Days Float	$0.00
YTD Interest Earned	$1,776.48
Interest Rate	1.000%

back to top

Exhibit 12

Federal Financial Institutions Examination Council

Exhibit 13

3501 Fairfax Drive • Room B7081a • Arlington, VA 22226-3550 • (703) 516-5588 • FAX (703) 562-6446 • http://www.ffiec.gov

Supplement to Authentication in an Internet Banking Environment

Purpose

On October 12, 2005, the FFIEC agencies[1] (Agencies) issued guidance entitled *Authentication in an Internet Banking Environment* (2005 Guidance or Guidance).[2] The 2005 Guidance provided a risk management framework for financial institutions offering Internet-based products and services to their customers. It stated that institutions should use effective methods to authenticate the identity of customers and that the techniques employed should be commensurate with the risks associated with the products and services offered and the protection of sensitive customer information. The Guidance provided minimum supervisory expectations for effective authentication controls applicable to high-risk online transactions involving access to customer information or the movement of funds to other parties. The 2005 Guidance also provided that institutions should perform periodic risk assessments and adjust their control mechanisms as appropriate in response to changing internal and external threats.

The purpose of this Supplement to the 2005 Guidance (Supplement) is to reinforce the Guidance's risk management framework and update the Agencies' expectations regarding customer authentication, layered security, or other controls in the increasingly hostile online environment. The Supplement reiterates and reinforces the expectations described in the 2005 Guidance that financial institutions should perform periodic risk assessments considering new and evolving threats to online accounts and adjust their customer authentication, layered security, and other controls as appropriate in response to identified risks. It establishes minimum control expectations for certain online banking activities and identifies controls that are less effective in the current environment. It also identifies certain specific minimum elements that should be part of an institution's customer awareness and education program.

---

[1] Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

[2] FRS SR Letter 05-19, October 13, 2005; FDIC Financial Institution Letter 103-2005, October 12, 2005; NCUA Letter to Credit Unions 05-CU-18, November 2005; OCC Bulletin 2005-35, October 2005; OTS CEO Memorandum 228, October 12, 2005.

Background

Since 2005, there have been significant changes in the threat landscape. Fraudsters have continued to develop and deploy more sophisticated, effective, and malicious methods to compromise authentication mechanisms and gain unauthorized access to customers' online accounts. Rapidly growing organized criminal groups have become more specialized in financial fraud and have been successful in compromising an increasing array of controls. Various complicated types of attack tools have been developed and automated into downloadable kits, increasing availability and permitting their use by less experienced fraudsters. Rootkit-based malware surreptitiously installed on a personal computer (PC) can monitor a customer's activities and facilitate the theft and misuse of their login credentials. Such malware can compromise some of the most robust online authentication techniques, including some forms of multi-factor authentication. Cyber crime complaints have risen substantially each year since 2005, particularly with respect to commercial accounts. Fraudsters are responsible for losses of hundreds of millions of dollars resulting from online account takeovers and unauthorized funds transfers.[3]

The Agencies are concerned that customer authentication methods and controls implemented in conformance with the Guidance several years ago have become less effective. Hence, the institution and its customers may face significant risk where periodic risk assessments and appropriate control enhancements have not routinely occurred.

General Supervisory Expectations

The concept of customer authentication, as described in the 2005 Guidance, is broad. It includes more than the initial authentication of the customer when he/she connects to the financial institution at login. Since virtually every authentication technique can be compromised, financial institutions should not rely solely on any single control for authorizing high risk transactions, but rather institute a system of layered security, as described herein.

---

[3] See IC3 Annual Internet Crime Reports 2005-2009.

Specific Supervisory Expectations

Risk Assessments

The Agencies reiterate and stress the expectation described in the 2005 Guidance that financial institutions should perform periodic risk assessments and adjust their customer authentication controls as appropriate in response to new threats to customers' online accounts. Financial institutions should review and update their existing risk assessments as new information becomes available, prior to implementing new electronic financial services, or at least every twelve months.[4] Updated risk assessments should consider, but not be limited to, the following factors:

- changes in the internal and external threat environment, including those discussed in the Appendix to this Supplement;
- changes in the customer base adopting electronic banking;
- changes in the customer functionality offered through electronic banking; and
- actual incidents of security breaches, identity theft, or fraud experienced by the institution or industry.

Customer Authentication for High-Risk Transactions

The 2005 Guidance's definition of "high-risk transactions" remains unchanged, i.e., electronic transactions involving access to customer information or the movement of funds to other parties. However, since 2005, more customers (both consumers and businesses) are conducting online transactions. The Agencies believe that it is prudent to recognize and address the fact that not every online transaction poses the same level of risk. Therefore, financial institutions should implement more robust controls as the risk level of the transaction increases.

Retail/Consumer Banking

Online consumer transactions generally involve accessing account information, bill payment, intrabank funds transfers, and occasional interbank funds transfers or wire transfers. Since the frequency and dollar amounts of these transactions are generally lower than commercial transactions, they pose a comparatively lower level of risk. Financial institutions should implement layered security, as described herein, consistent with the risk for covered consumer transactions.

---

[4] See *FFIEC IT Examination Handbook*, Information Security Booklet, July 2006, Key Risk Assessment Practices section.

Business/Commercial Banking

Online business transactions generally involve ACH file origination and frequent interbank wire transfers. Since the frequency and dollar amounts of these transactions are generally higher than consumer transactions, they pose a comparatively increased level of risk to the institution and its customer. Financial institutions should implement layered security, as described herein, utilizing controls consistent with the increased level of risk for covered business transactions. Additionally, the Agencies recommend that institutions offer multifactor authentication to their business customers.

Layered Security Programs

Layered security is characterized by the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control. Layered security can substantially strengthen the overall security of Internet-based services and be effective in protecting sensitive customer information, preventing identity theft, and reducing account takeovers and the resulting financial losses. It should be noted that other regulations and guidelines also specifically address financial institutions' responsibilities to protect customer information and prevent identity theft.[5] Financial institutions should implement a layered approach to security for high-risk Internet-based systems.[6]

Effective controls that may be included in a layered security program include, but are not limited to:

- fraud detection and monitoring systems that include consideration of customer history and behavior and enable a timely and effective institution response;
- the use of dual customer authorization through different access devices;
- the use of out-of-band verification for transactions;
- the use of "positive pay," debit blocks, and other techniques to appropriately limit the transactional use of the account;

[5] See Interagency Final Regulation and Guidelines on Identity Theft Red Flags, 12 CFR parts 41, 222, 334, 571, and 717; Interagency Guidelines Establishing Information Security Standards, 12 CFR parts 30, 208, 225, 364, and 570, Appendix B.
[6] See *FFIEC IT Examination Handbook*, Information Security Booklet, July 2006, Key Concepts section.

- enhanced controls over account activities; such as transaction value thresholds, payment recipients, number of transactions allowed per day, and allowable payment windows (e.g., days and times);
- internet protocol (IP) reputation-based tools to block connection to banking servers from IP addresses known or suspected to be associated with fraudulent activities;
- policies and practices for addressing customer devices identified as potentially compromised and customers who may be facilitating fraud;
- enhanced control over changes to account maintenance activities performed by customers either online or through customer service channels; and
- enhanced customer education to increase awareness of the fraud risk and effective techniques customers can use to mitigate the risk.

The Agencies expect that an institution's layered security program will contain the following two elements, at a minimum.

<u>Detect and Respond to Suspicious Activity</u>

Layered security controls should include processes designed to detect anomalies and effectively respond to suspicious or anomalous activity related to:

- initial login and authentication of customers requesting access to the institution's electronic banking system; and
- initiation of electronic transactions involving the transfer of funds to other parties.

Based upon the incidents the Agencies have reviewed, manual or automated transaction monitoring or anomaly detection and response could have prevented many of the frauds since the ACH/wire transfers being originated by the fraudsters were anomalous when compared with the customer's established patterns of behavior.

<u>Control of Administrative Functions</u>

For business accounts, layered security should include enhanced controls for system administrators who are granted privileges to set up or change system configurations, such as setting access privileges and application configurations and/or limitations. These enhanced controls should exceed the controls applicable to routine business customer users. For example, a preventive control could include requiring an additional authentication routine or a transaction verification routine prior to final implementation of the access or application changes. An example of a detective control could include a transaction verification notice

immediately following implementation of the submitted access or application changes. As discussed in the Appendix, out-of-band authentication, verification, or alerting can be effective controls. Based upon the incidents the Agencies have reviewed, enhanced controls over administrative access and functions can effectively reduce money transfer fraud.

Effectiveness of Certain Authentication Techniques

Device Identification

In response to the 2005 Guidance, many financial institutions implemented simple device identification. This typically uses a cookie loaded on the customer's PC to confirm that it is the same PC that was enrolled by the customer and matches the logon ID and password that is being provided. However, experience has shown this type of cookie may be copied and moved to a fraudster's PC, allowing the fraudster to impersonate the legitimate customer. Device identification has also been implemented using geo-location or Internet protocol address matching. However, increasing evidence has shown that fraudsters often use proxies, which allow them to hide their actual location and pretend to be the legitimate user.[7]

Simple device identification as described above can be distinguished from a more sophisticated form of this technique which uses "one-time" cookies and creates a more complex digital "fingerprint" by looking at a number of characteristics including PC configuration, Internet protocol address, geo-location, and other factors.[8] Although no device authentication method can mitigate all threats, the Agencies consider complex device identification to be more secure and preferable to simple device identification. Institutions should no longer consider simple device identification, as a primary control, to be an effective risk mitigation technique.

Challenge Questions

Many institutions use challenge questions as a backup in the event that the primary logon authentication technique becomes inoperable or presents an unexpected characteristic. The provision of correct responses to challenge questions can also be used to re-authenticate the customer or verify a specific transaction subsequent to the initial logon. Similar to device identification,

---

[7] The National Security Agency has developed a patented method, available for public licensing, that can detect the use of a proxy.

[8] Technology vendors have developed "one-time" cookies which expire if stolen from the PC onto which they were originally loaded.

challenge questions can be implemented in a variety of ways that impact their effectiveness as an authentication tool. In its basic form, the user is presented with one or more simple questions from a list that was first presented to the customer when they originally enrolled in the online banking system. These questions can often be easily answered by an impostor who knows the customer or has used an Internet search engine to get information about the customer (e.g., mother's maiden name, high school the customer graduated from, year of graduation from college, etc.). In view of the amount of information about people that is readily available on the Internet and the information that individuals themselves make available on social networking websites, institutions should no longer consider such basic challenge questions, as a primary control, to be an effective risk mitigation technique.

Challenge questions can be implemented more effectively using sophisticated questions. These are commonly referred to as "out of wallet" questions, that do not rely on information that is often publicly available. They are much more difficult for an impostor to answer correctly. Sophisticated challenge question systems usually require that the customer correctly answer more than one question and often include a "red herring" question that is designed to trick the fraudster, but which the legitimate customer will recognize as nonsensical. The Agencies have also found that the number of challenge questions employed has a significant impact on the effectiveness of this control. Solutions that use multiple challenge questions, without exposing all the questions in one session, are more effective. Although no challenge question method can mitigate all threats, the Agencies believe the use of sophisticated questions as described above can be an effective component of a layered security program.

Customer Awareness and Education

A financial institution's customer awareness and educational efforts should address both retail and commercial account holders and, at a minimum, include the following elements:

- An explanation of protections provided, and not provided, to account holders relative to electronic funds transfers under Regulation E, and a related explanation of the applicability of Regulation E to the types of accounts with Internet access;
- An explanation of under what, if any, circumstances and through what means the institution may contact a customer on an unsolicited basis and request the customer's provision of electronic banking credentials;
- A suggestion that commercial online banking customers perform a related risk assessment and controls evaluation periodically;

- A listing of alternative risk control mechanisms that customers may consider implementing to mitigate their own risk, or alternatively, a listing of available resources where such information can be found; and,
- A listing of institutional contacts for customers' discretionary use in the event they notice suspicious account activity or experience customer information security-related events.

The attached Appendix contains an additional discussion of online threats and control methods.

Appendix

Threat Landscape and Compensating Controls

Threats

As noted previously in this Supplement, the Agencies are concerned that fraudsters are utilizing increasingly sophisticated and malicious techniques to thwart existing authentication controls, gain control of customer accounts, and transfer funds to money mules that facilitate the movement of those funds beyond the reach of financial institutions and law enforcement. Many of these schemes target small to medium-sized business customers since their account balances are generally higher than consumer accounts and their transaction activity is generally greater making it easier to hide the fraudulent transfers.

An effective tool in the fraudster's arsenal is keylogging malware. A keylogger is a software program that records the keystrokes entered on the PC on which it is installed and transmits a record of those keystrokes to the person controlling the malware over the Internet. Keyloggers can be surreptitiously installed on a PC by simply visiting an infected website or by clicking on an infected website banner advertisement or email attachment. Keylogging can also be accomplished via a hardware device plugged into the PC which stores the captured data for later use. Keylogger files are generally small in size and adept at hiding themselves on the user's PC. They often go undetected by most antivirus programs. Fraudsters use keyloggers to steal the logon ID, password, and challenge question answers of financial institution customers. This information alone or in conjunction with stolen browser cookies loaded on the fraudster's PC may enable the fraudster to log into the customer's account and transfer funds to accounts controlled by the fraudster, usually through wire or ACH transactions.

Other types of more sophisticated malware allow fraudsters to perpetrate man-in-the middle (MIM) or man-in-the browser (MIB) attacks on their victims. In a MIM/MIB attack, the fraudster inserts himself between the customer and the financial institution and hijacks the online session. In one scenario, the fraudster is able to intercept the authentication credentials submitted by the customer and log into the customer's account. In another scenario, the fraudster does not intercept the credentials, but modifies the transaction content or inserts additional transactions not authorized by the customer which, in most cases, are funds transfers to accounts controlled by the fraudster. The fraudsters conceal their actions by directing the customer to a fraudulent website that is a mirror image of

the financial institution's website or sending the customer a message claiming that the institution's website is unavailable and to try again later. Fraudsters may have the capacity to delete any trace of their attack from the log files.

MIM/MIB attacks may be used to circumvent some strong authentication methods and other controls, including one-time password (OTP) tokens. OTP tokens have been used for several years and have been considered to be one of the stronger authentication technologies in use. Since the one-time password is generally only good for 30-60 seconds after it is generated, the fraudster must intercept and use it in real time in order to compromise the customer's account.

Controls

The Agencies are aware of a variety of security techniques which can be used to help detect and prevent the types of attacks described above. Some of these techniques have been in use for some time, while others are relatively new. Financial institutions should investigate which of these controls may be more effective in detecting and preventing attacks as part of the institution's layered security program. However, it is important to note, that none of the controls discussed provide absolute assurance in preventing or detecting a successful attack. These controls may include the following:

Anti-malware software may provide a defense against keyloggers and MIM/MIB attacks. Anti-malware is a term that is commonly used to describe various software products that may also be referred to as anti-virus or anti-spyware. Anti-malware software is used to prevent, detect, block, and remove adware, spyware, and other forms of malware such as keyloggers. It is important to note that anti-malware is generally signature based, and some advanced versions of malware continuously alter their signature.

Transaction monitoring/anomaly detection software has been in use for a number of years. Similar to the manner in which the credit card industry detects and blocks fraudulent credit card transactions, systems are now available to monitor online banking activity for suspicious funds transfers. They can stop a suspicious ACH/wire transfer before completion and alert the institution and/or the customer so that the transfer can be further authenticated or dropped. Based upon the incidents the Agencies have reviewed, manual or automated transaction monitoring/anomaly detection could have assisted in preventing many fraudulent money transfers as they were clearly out of the ordinary when compared with the customer's established patterns of behavior. Automated systems may also look at the velocity of a transaction and other similar factors to determine whether it is suspicious.

The Agencies are aware of the fact that a number of institutions are requiring the "out-of-band" authentication or verification of certain high value and/or anomalous transactions. Out-of-band authentication means that a transaction that is initiated via one delivery channel (e.g., Internet) must be re-authenticated or verified via an independent delivery channel (e.g., telephone) in order for the transaction to be completed. Out-of-band authentication is becoming more popular given that customer PCs are increasingly vulnerable to malware attacks. However, out-of-band authentication directed to or input through the same device that initiates the transaction may not be effective since that device may have been compromised. For business customers, the out-of-band authentication or verification can be provided by someone other than the person who first initiated the transaction and can be combined with other administrative controls. Additionally, the use of out-of-band authentication or verification, for administrative changes to online business accounts, can be an effective control to reduce fraudulent funds transfers.

In response to the rising malware infection rates of customer PCs, a number of vendors have developed USB devices that increase session security when plugged into the customer's PC. These devices can function in several ways, but they generally enable a secure link between the customer's PC and the financial institution independent of the PC's operating system and application software. Typically, the device's firmware is "read only" and cannot be altered by the customer or the malware infecting the PC.

The use of restricted funds transfer recipient lists or other controls over the administration of such lists, can reduce funds transfer fraud. Fraudsters must frequently add new funds transfer recipients to an account profile in order to consummate the fraud.

Overall, the Agencies agree with security experts who believe that institutions should no longer rely on one form of customer authentication. A one dimensional customer authentication program is simply not robust enough to provide the level of security that customers expect and that protects institutions from financial and reputation risk. This concept of layered security is consistent with expectations the Agencies have discussed previously.[9] Layered security controls do not have to be complex. For example, implementing time of day restrictions on the customer's authority to execute funds transfers or using restricted funds transfer recipient

[9] See *FFIEC IT Examination Handbook*, Information Security Booklet, July 2006; FFIEC IT Examination Handbook, E-Banking Booklet, August 2003.

lists, in addition to robust logon authentication, can help to reduce the possibility of fraud.

The banking, payment, and security industries have continued to innovate in response to the increasing cyber threat environment. In addition to some of the control methods previously discussed, other examples of customer authentication include keystroke dynamics and biometric based responses. Additionally, institutions can look to traditional and innovative business process controls to improve security over customers' online activities. Some examples include:

- establish, require and periodically review volume and value limitations or parameters for what activities a business customer in the aggregate, and its enrolled users individually, can functionally accomplish while accessing the online system;
- monitor and alert on exception events;
- establish individual transaction and aggregate account exposure limits based on expected account activity;
- establish payee whitelisting (e.g., positive pay) and/or blacklisting;
- require every ACH file originating entity to provide a proactive notice of intent to originate a file prior to its submission; and
- require business customers to deploy dual control routines over higher risk functions performed online.